Accountants' acceptance of a cashless monetary system using an implantable chip

Antony Michael Young
Bachelor of Business (Accounting), Swinburne Institute of Technology
Post Graduate Diploma of Education, Latrobe University
Master of Accounting, University of New England

A thesis submitted to RMIT University for the fulfilment of the degree of Doctor of Philosophy (PhD.)
July 2007

Acknowledgements

Firstly I want to give a special thanks to my loving wife Ann for her sacrifices during the duration of my PhD and her support, especially her interest in the issues of the thesis. I also want to thank my children, Jacinta, Kurtis and Chontelle who never complained when I worked on the thesis rather than played with them. I want to acknowledge my appreciation to my Father and Mother for the loving way they supported my intellectual inquiry as I grew.

Academically I want to thank Professor Robert Clift for the support he showed me in the development of this thesis. His direction and support was fundamental in its development. I also want to thank my second supervisor Doctor David Gowland for his valuable contributions, support and patience. A special note of thanks to Professor Clive Morley who generously devoted time and effort to provide guidance on the statistical interpretations contained within this PhD.

Abstract

A logical control extension surrounding cashless means of exchange is a permanent personal verification mark. An implanted micro chip such as ones that have been successfully implanted into humans could identify and store information. Connected with global positioning satellites and a computer system, a cashless monetary system could be formed in the future. The system would provide complete and continual real time records for individuals, businesses and regulators. It would be possible for all trading to occur in this way in the future. A modified Technology Acceptance Model was developed based on Davis' (1989) model and Fishbein and Ajzen's (1975) theory to test the acceptance level of the new monetary system by professional accountants in Australia. The model includes perceived ease of use, perceived usefulness, perceived risk, and a subjective norm component. 523 accountants were surveyed in December 2003 with a response rate of 27%. 13% either strongly agreed or agreed that they would accept the implantable chip. The analysis showed that Perception of Risk, Subjective Norm and Perception of Usefulness were all significant in explaining the dependent variable at the 95% confidence level for all responses. The Perception of Ease of Use was not proved to be significant. In consideration of response bias, it was found that with respect to the perception of usefulness at the 0.01 level, two elements were not significant, those being "not having cards" and "having medical information". The difference here was not seen as fundamental for the credibility of the research given the main theme of the research is a monetary system based on the "mark" rather than the convenience factors of the two elements where there were differences. The perceived risk variable was not significant for early responders. The responses were also used to analyse the Technology Acceptance Model developed by Davis (1989). The model had a significance of 0.327

compared to 0.000 giving validation to the contributions of the modified Technology Acceptance Model. Davis' (1989) model found Perception of Ease of Use was significant at the 95% confidence level and Perception of Usefulness was not proven to be significant. In further analyzing the developed model, each of the elements in the model used as independent variables were separately regressed against contributions established in open questions relating to them. Subjective norm had a regression R-squared of 0.403 and of the thirty-four explanatory variables the only significant contribution, at the 95% confidence level was "clients". Significant at the 10% level, were religion, public figures and friends. The professional bodies variable was not significant in determining the subjective norm. Perceived Ease of Use and the nine explanatory variables had an R-squared of 0.143. There were only two significant contributions for ease of use, at the 95% confidence level being "privacy" and "technology". Perceived Usefulness and the eleven explanatory variables had an R-squared of 0.205. There were only two significant contributions for usefulness, at the 95% confidence level being "privacy" and "easy". Perceived Risk and the eleven explanatory variables had an R-squared of 0.054 and no significant contributions.

Declaration

Except where reference is made in the text, this thesis contains no material published elsewhere or extracted in whole or in part from this thesis presented by me for another degree or diploma.

No other person's work has been used without acknowledgment in the main text of this thesis.

This thesis has not been submitted for the award of any degree or diploma in any other tertiary institution.

Antony Young

TABLE OF CONTENT

APPENDICES

1. Descriptive statistics

4. **Perceived usefulness (open question)**
    - **4.1 Medical issues**
    - **4.2 Identity issues**
    - **4.3 Security issues**
    - **4.4 Recording issues**
    - **4.5 Access issues**
    - **4.6 Ease issues**
    - **4.7 Problems**
    - **4.8 Privacy issues**
    - **4.9 Protest issues**
    - **4.10 Fraud issues**
    - **4.11 Taxation issues**
5. **Perceived risk (control – open question)**
    - **5.1 Privacy issues**
    - **5.2 Control issues**
    - **5.3 Misuse issues**
    - **5.4 Marketing issues**
    - **5.5 Rights issues**
    - **5.6 Physical safety issues**
    - **5.7 Management issues**
6. **"Other" Risks (open question)**
    - **6.1 Misuse issues**
    - **6.2 Control issues**
    - **6.3 Health issues**
    - **6.4 Technology issues**
    - **6.5 Privacy issues**
    - **6.6 Identity issues**
7. **Factors affecting acceptance (open – question)**
    - **7.1 Control issues**
    - **7.2 Privacy issues**
    - **7.3 Technology issues**
    - **7.4 Misuse issues**
    - **7.5 Health issues**

LIST OF CHARTS

LIST OF TABLES

LIST OF GRAPHS

Chapter One: Introduction

1.1 Introduction

1.1.1 Research introduced

Professional accountants are trained to deal with change. Their opinions are sought in new uncertain financial circumstances such as an emerging taxation system. This research solicits accountants' views of accepting an emerging cashless monetary system. The system revolves around microchips implanted into humans accessed by individual scanners and embracing global positioning satellites supported by computers which record transactions. A person would present their implanted microchip (referred to as a verification mark) which would most likely be implanted in their wrist to the scanner which would scan the microchip in the same way a barcode of a product is scanned at a supermarket. The scanner would make a transfer of the amount agreed should sufficient funds or credit allow, otherwise it would be disallowed and an error message would be displayed on the scanner. Personal monetary exchanges would happen in the same way using small portable scanners normally part of a mobile phone. The debits or credits in a person's bank account would be updated in real time on the central computer via satellite.

1.1.2 Cashless monetary systems explained

A cashless monetary exchange does not use a physical or tangible token of exchange (including cash such as an Australian coin or note) in the fulfilment of a financial transaction. In the simplest form a cashless medium of exchange can be represented by an isolated payment method without the need for cash such as a store value card for the payment of a particular service.

Cashless mediums of exchange can also be part of a more sophisticated payment system such as the use of credit cards either over the counter, online or over the phone. The less need there is for physical forms of cash for transactions the more sophisticated the cashless system is seen to be.

The cashless monetary system envisaged by this research examines a system that does not require any cash whatsoever. A microchip would be implanted into every person's body complemented by infrastructure in place so that every person had the hardware to pass and receive exchanges of wealth via a scanner that would be carried in a similar way that a wallet, purse or a mobile phone might be carried currently. The implanted chip and scanner would eliminate the financial and identity need for a purse or wallet. As an example the scanner could be conveniently placed in a mobile phone so that it was not additionally needed beyond what a person might usually carry with them. The scanner would require a person's implanted chip to activate it, so it would become useless without the person. Should a forced robbery occur, making use of the person and their chip, the destination of the funds could be easily traced and subsequently followed up by police who could reverse the entry and make arrests regarding the crime.

1.1.3 Factors driving a cashless monetary system

1.1.3.1 Perceived need to reduce fraud

The purpose of the following sections is to demonstrate that with a sophisticating society, there is a movement toward a cashless monetary system. The trend is firstly driven by a perceived need to reduce fraud. Secondly the development of various components of the technology enables the system to become a reality.

The existence of cash transactions has allowed money laundering to become a large issue, prompting planned changes to eliminate cash transactions to ensure transfers are traceable. The Federal government on 13 July 2006 released the Anti-Money Laundering and Counter-Terrorism Financing Bill. The proposed bill will bring Australia in line with international standards issued by the Financial Task Force on Money Laundering up-dating the Financial Transaction Reports Act 1988 which was developed to control money laundering (http://www.cpaaustralia.com.au/cps/rde/xchg/cpa/hs.xsl/1017_19312_ENA_HTML.htm, accessed on 1st September 2006). Until a single identifier and an audit trail which traces to an individual has been developed it will remain a problem. According to the Financial Action Task Force on money laundering, "a key element in the fight against money laundering and the financing of terrorism is the need for countries' systems to be monitored and evaluated" (Strasser 1998, p. 1). International standards have been developed which will be assessed by the International Monetary Fund and World Bank (Strasser 1998).

The cost of money laundering and over a billion dollars of identity fraud exists in Australia alone. The government is bearing much of this burden as significant amounts are linked to welfare fraud, and they are very keen to find a solution and are even considering biometric solutions. The world agenda on terrorism is also driving non-removable individual identification. An implantable chip using biometric identification processes provides an auditable number.

Businesses also have motivation to drive non-removable identity numbers via a cashless monetary system. For example, the banking industry is keen to eliminate their liability for fraud, while retail environments are also seeking to reduce the amount of consumer theft they are encountering.

The banking "industry is facing combined losses of more than $100 million in credit card fraud alone" and are seeking solutions (Connors et al 2005, p. 1). For example, "Westpac has held high-level discussions with its competitors and it expects customers to be using their fingerprint, face or some other form of biometric identification to access Internet banking within the next 18 months" (Connors et al 2005, p. 1). The new technology is being adopted internationally by Europay, Mastercard and Visa.

According to Moullakis (2005), there are legal ramifications for banks not adopting microchip based technology.

> "Without the newer computer chip-based technology, banks will be liable for fraud perpetrated regardless of whether they issued the card, processed the transaction or the purchase was made locally or overseas" (p. 68).

There are many reasons driving the compulsory use of such a monetary system. One of which being the importance of using the chips to enhance identity controls. Attorney-General, Philip Ruddock MP, in the opening keynote address to Australian Smart Cards Summit (2005), indicated the identity fraud as a serious threat to business community particularly in electronic commerce.

> "The Australian Bankers' Association estimates the cost to the banking industry at $25 million a year. And two years ago Austrac estimated the annual cost of identity crime in Australia at $1.1 billion. Globally, we are looking at a figure as high as $2 trillion" (Opening keynote address to Australian Smart Cards Summit 2005, available: http://www.ag.gov.au/agd/WWW/MinisterRuddockHome.nsf/Page/Speeches_2005_Speeches_29_June_2005_Speech_Opening_Keynote_Address_to_Australian_Smart_Cards_Summit_2005, accessed on 3rd November 2006).

Identity fraud costs Australia about $1.1 billion annually according to Moullakis (2005). Tinkler (2006) also documents that estimates of "identity and credit card fraud costs the country about $1.1 billion a year" (p. 17).

Moor (2002, p. 1) notes that "law enforcers want every Australian to be finger or eye scanned "to counter" the identity fraud crisis. The unique identifiers would be stored on a government database". Proposed uses would be for those "seeking welfare payments – or applying for documents such as passports or driving licences" Moor (2002, p. 1).

The government are pursuing biometric and identity card solutions, which are advertised as voluntary for anyone wishing to receive welfare support. Compulsory identity cards

are currently being proposed for anyone wishing to receive welfare. Henry (2006) documents that government tenders have been calling for the trials to a new ID smart card. "The access card is expected to replace 17 health and social services cards and vouchers, including the Medicare card" (p. 1). "One of those tenders states that the trials for the new ID Smart card will begin in 2008 for full implementation during 2010". The Australian Law Reform Commission (2006), in Issue Paper 31 - Review of Privacy, addresses as the issue of the "Multi-Purpose Identifiers", referred to as "The Access Card" (section 12-42).

The Australian Law Reform Commission, Issue Paper 31 states:

> "The Access Card will replace 17 existing health care and social services cards and vouchers. It will display the cardholder's name and photograph on its front, and the cardholder's signature and card number on its back. The card number will be the cardholder's current Medicare number, reformatted with extra digits where necessary to ensure it is unique. Other personal information, such as the cardholder's photograph, address, date of birth, concession status, and details of the cardholder's children or dependants will be stored on a microchip embedded in the card. The cardholder may also choose to store further information on the card's chip, such as 'emergency contact details, allergies, health alerts, chronic illnesses, immunisation information or organ donor status'". (Section 12.42)
>
> "Registration for the card is scheduled to commence in 2008 and conclude in early 2010, after which a card will be required in order to access any health or social services". (Section 12.43)

Michael et al (2005, p. 22) note that "more sophisticated auto-ID devices like smart card and radio-frequency identification (RFID) tags and transponders that house unique

lifetime identifiers or biometric templates" are being considered for transactions between businesses and their consumers and by governments and citizens. An implantable chip is a microchip, which can be implanted into a person's body such as those currently in use, which use radio frequency to allow external identification. The components of the described cashless monetary system are currently in use.

1.1.3.2 Current availability of technology

Johnston (2005) in examining technology used by accountants predicts that soon "nearly every CPA will need to understand" (p. 96) RFID (radio frequency identification). Strasser (1998) contributes that "advances in encryption and computer networks have paved the way for a purely electronic-based currency substitute: digital money" (p. 1).

According to Phillips G. (2004):

> "chip implants seem to be catching on", "and the day mightn't be far away when you'll be having yourself computerised. Indeed the day mightn't be far away when it becomes compulsory, to help in the fight against terrorism" (p. 21).

Supermarket chains in the United Kingdom are using the radio-frequency identification (RFID) chips to reduce shoplifting (Engberg et al 2004, p. 89). Trials have also been carried out in Australia (Houghton et al 2005, p. 77).

"Britain has announced that it is considering implanting illegal immigrants with RFID transponders (Michael et al 2005, p. 22) allowing them to be constantly traced by global positioning satellites. Internationally, "countries are taking measures against fraudulent

claims made on social security with more secure end-user devices" (Michael et al 2005, p. 22).

> "Visa is piloting the service in Japan with Telco NTT DoCoMo where phone subscribers download a soft version of their credit card's details or insert a SIM-size chip into special m-commerce phones. These beam payments to infra-red ports attached to terminals at selected merchants" (Timson 2003, p. 7 - 9).

In Australia mobile phones are currently being used as an electronic wallet for payment of such items as soft drinks and parking meters.

Mastercard also uses a Pay Pass that uses a chip, which uses radio frequency readers that receive the card's signals and transmits them to the terminal. "Security remains a big concern" (Timson 2003, p. 7) and implanting the chip could solve at least part of the problem of lost phones.

Smartcards are increasingly common in our society. Recently a "smartcard giving tourists access to more than 60 of Victoria's best attractions" was offered for sale (Metlikovec 2003, p. 17).

"Already customers of South Korea's department stores can pay for purchases on credit cards by waving their mobile phones at payment terminals" (Timson 2003, p. 7). Any third generation mobile phone could carry a number of tokens or smartcards, including one for a public key infrastructure authentication certificate, all separated by firewalls. A recent survey found "10 percent of mobile phone users were interested in banking with

their phones" (Timson 2003, p. 7). Mastercard are testing the system in Texas with Nokia.

1.1.3.3 Summary

In summary, there are enormous motivations for the international community's war on terrorism and money laundry to adopt unique identity controls. The cost of fraud on businesses and the government highly motivates a move towards a traceable cashless monetary system. The technology supporting a cashless monetary system based on implantable chips is developing at a rapid rate. Microchips implanted in humans are currently being used for various applications including the identification and tracking via global positioning satellite of sex offenders. Computer networks are currently sophisticated enough to handle the volume of transactions required in the described cashless monetary system. Development in data protection processes including encryption software are sufficiently developed for use in the system and are becoming increasingly advanced. Biometric solutions are currently being used matched with an individual and accessible identity number via an implantable chip.

1.2 Motivation for the study

There is evidence of a move towards cashless systems of exchange. The long-term goal of the Swedish cash card system "is to replace cash" (Holmstrom and Stalder 2001, p. 190), "the short term goal; is to offer an alternative means of payment in places where cash is prevalent, for example, in small shops and on buses". Michael et al (2005, p. 23) reports that

> "we are witnessing the transition period in which auto-ID devices especially are being trialled upon those who either desperately require their use for medical purposes, or cannot challenge their application, such as in the case of armed forces or prison inmates. Eventually, the new technology will be opened to the wider market in a voluntary way but will become a de facto compulsory standard (such as with the mobile phone today), and inevitably mandatory as it is linked to some kind of requirement for survival. This is the pattern that most successful high-tech innovations throughout history have followed".

Consider a situation where the Australian dollar loses its value due to a catastrophic event in the market. People who have lost their purchasing power may be very keen to adopt a system that re-established their wealth and may be more likely to accept a solution such as a cashless monetary system based on implantable chips than those without the loss of value of the currency. An international currency may replace the Australian dollar in conjunction with cashless system. This may occur in a similar manner to how the Euro was adopted. Especially with self-funded retirement, the lifestyles of people in Australia are very attached to their assets and would be vulnerable

to requirements to re-establish their wealth. Cashless monetary systems with a new currency may become the logical solution to re-establish monetary value to people.

The cashless system described revolves around permanent identification via chip implants. Referring to a prediction made by a Franklin Piece Law Centre report, Michael et al (2005, p. 25) note that:

> "A national identification system via microchip implants could be achieved in two stages: Upon introduction as a voluntary system, the microchip implantation will appear to be palatable. After there is a familiarity with the procedure and knowledge of its benefits, implantation would be mandatory".

In the United Kingdom on 14 February 2006 the government introduced the Chip and PIN programme, which requires that

> "cardholders must use their PIN to be sure of being able to pay with their chip and PIN card. If shoppers don't use PIN, their card may be declined and the option of signing can no longer be guaranteed" (http://www.chipandpin.co.uk/reflib/chipandpin_10oct05.pdf, accessed 13th May 2006).

> "There will still be some instances where cardholders will continue to sign even after 14 February 2006. These include:
>
> - Purchases in outlets which are not yet using chip and PIN technology
> - Purchases made on cards which have not yet been upgraded to chip and PIN
> - Disabled customers using a chip and signature card instead of a chip and PIN card will always continue to sign" (http://www.chipandpin.co.uk/reflib/chipandpin_10oct05.pdf, accessed 13th May 2006).

Chips are becoming more commonplace with the federal government "set to introduce new Australian passports which will include electronic identity chips. The chips will carry biometric fingerprints-iris and retinal images and details of the holder's hand geometry" (Haberfield 2003, p. 2). The US Congress in 2002 approved legislation requiring passports that could store fingerprints, iris scans and other biometric identifiers.

Morrissey (2005) reports that an Australian football team based in Sydney has adopted technology which uses a global positioning satellite system in an attempt to monitor how the players are performing. "Players are wearing a GPS locator the size of a mobile phone strapped to their backs linking them to several satellites above Australia" (p. 35).

Traceable chips may also become part of "a high-tech attack on cheating" which would allow federal police to investigate an extra 1200 identity fraud cases each year (Wallace 2003 p. 14).

Phillips, G. (2004, p. 21) in contemplation of compulsory chip implantation being unthinkable makes the point that so also was

> "the idea of compulsory fingerprinting and face scanning a few years ago. Yet, that now happens to anyone who wants to visit America – in the name of the fight against terrorism".

The observance of sophisticated cashless forms of exchange, the proliferation of these forms of exchange and the move towards compulsory identity checks led me to consider Revelation 13:16-17 which could be seen as a reference to a cashless society:

> "everyone, small and great, rich and poor, free and slave, receive a mark on his right hand or the forehead, so that no one can buy or sell unless he has the mark…..".

Making use of global positioning satellites, emerging technological and communication capacities a monetary system could develop and facilitate a cashless society and so it is deemed important and appropriate to discuss what professional accountants thought of the prospect.

1.3 The development of cashless mediums of exchange

This research can be justified on the basis of the rapid development of cashless mediums of exchange world wide and the need to study effects on personal rights. This section presents the definition of money and then proceeds to consider various forms of cashless mediums of exchange including electronic banking, electronic cash and smart cards. The legal aspects of money are also considered in the context of a cashless society.

1.3.1 Defining money

Solomon (1991, p 15) defines money as:

> “a form of value generally acceptable in payments of goods and services. It ought also to serve as a unit of account and a medium for storing value effectively”.

Crowley (1995), on the other hand, defines money as:

> "the store of purchasing power universally used and generally accepted by the public in the settlement of economic transactions. It allows the purchase of goods and services and the settlement of financial transactions to proceed with minimal effort and cost" (p. 2).

He states:

> "essential properties which money must have to carry out tasks include public confidence that money will hold its value in terms of purchasing power and that the issuers of money are prudentially sound" (p.15).

What has constituted a medium of exchange has changed considerably over time. What is clear, however, is that some system is necessary to place a value on exchange even if this is as simplistic as the rudimentary system of barter. The modern manifestations of barter are systems like "Barter card" (http://www.bartercard.com/au/page.asp?2083=501306&E_Page=79280&contentID=501306&parentcategory=501306, accessed on 30th November 2006). Using a plastic card, purchases of goods or services can be made in participating organisations with special "trade credit" which is an accumulation of wealth gained when a good or service is contributed to another within the scheme that allows the contributor the rights to that amount of goods or services from other participants in the system. Participants pay using the credit generated from the sale of their own products or services with a discount equivalent to the gross margin. The Barter Card's currency of a "Trade Dollar" is equal to one Australian Dollar for

accounting and tax purposes. The system extends to overseas locations where offices are available (http://www.bartercard.co.nz/index.asp?PageID=2145829501, accessed on 30th November 2006).

Originally the awkwardness of the barter system of exchange eventually led to physical forms of wealth and exchange, which then led to cash. Cash was previously linked to gold but now is related to monetary policy. Credit providers also contribute to the money supply and the diversity and volume of the offerings are increasing. The awkward non-cash alternatives such as cheques are being replaced by debit cards, credit cards and other more sophisticated forms of exchange. Niman (1985 p. 1) states, "technological developments are making possible the issue of money outside the traditional banking system".

As economies become more sophisticated, pressure is brought to bear on the system of exchange to reflect this. Technological improvements have allowed significant advances in the mediums of exchange including cashless varieties. Some economists model electronic money as "new types of barter" or "new types of money" or refer to it as "netting arrangements" (Green 1999, p. 668).

1.3.2 Electronic banking

Al-Hajri (2005) suggested in his PhD thesis: Internet Technology Adoption In The Banking Industry, a "strong banking industry supports economic developments significantly through its efficient financial service" (ii). In order to make the financial service sector efficient, banks are required to "introduce changes such as the banking

industry moving from traditional distribution channel banking to electronic distribution channel banking" (Al-Hajri 2005, p. ii), especially with fast growth of the modern technology, the need for using electronic banking is more obvious.

According to Bollen (2001) electronic banking can be divided into two categories, the first being "pure" which is "where no card, terminal or other proprietary device is needed". The second is called "hybrid" which is "using both an electronic network and physical tokens" (p. 6) such as a credit card.

For businesses, "the Internet enables much lower cost communication and processing, as a result many financial institutions have begun to offer various forms of electronic banking using Internet facilities" (Bollen 2001, p. 5). Some banks only provide such services, known as cyber banks. A "cyber bank may be no more than an operator with a computer and Internet connection" (Snedden 1997, p. 65). Mara (2000, p. 6) states, "the race is on to see which major Australian players' consolidate positions in the Internet market place before global institutions do."

If cashless forms of transactions are cheaper for financial institutions then financial incentives and disincentives will apply to clients to motivate them to use these forms. Already banks charge more to visit them in person. Niman (1985, p. 1) argues, "electronic impulses offer a lower cost alternative".

Convenience to the consumer is another major reason cashless forms of exchange are growing. For instance, Internet banking allows "consumers 24 hour access to their

accounts and greater control over fund transfers, especially those of an international nature" (Bollen 2001, p. 5).

1.3.3 Legal aspects of money

Crowley (1995) explains that "the creation and issue of money in Australia has, in the post-war period, been strictly limited to the Reserve Bank of Australia and the banks" (p. 2) which were strictly regulated. Legislation dealing with monetary systems has its history steeped in "deposit-taking and the creation of accounts".

Kreltszheim (2003) notes when examining the legal nature of electronic money that "given the embryonic nature of the new payment technologies, the legislators have – by and large-adopted a policy of 'technological neutrality' (p. 262). Specific references to the underlying technologies have not been used when defining the scope of the regulation, which apply to the new technologies. In the main, electronic payments have been considered "surrogates for coins and banknotes" (p. 264). There has also been a "marked desire not to impose undue regulatory burdens on prospective new entrants into the payment system industry" (p. 264).

1.3.4 Smart cards

Stored-value-cards have also developed and are becoming more common. These cards contain a silicon chip capable of storing large amounts of information interactively. Aardsma (2001 p. 12) defines them as "portable memory devices that can be used to

store and transfer information from central computers" and details that the smart cards are "equipped with a built-in microprocessor that supports more advanced information management and security methods".

Smart cards are being used as a substitute for cash and some suggest smart cards are indeed replacing cash (Ling 2001). Internet banking is likely to be linked to smart cards.

> "…these could include virtual Automatic Teller Machine (ATM) functions through the recharge of a consumer's smart card. That is, a consumer may be able to transfer funds from their account to their smart card using an Internet banking service and a unit attached to their personal computer capable of reading from and writing to the card…" (Bollen 2001, p. 7).

Microchip technology continues to develop in capacity and sophistication. Samsung Electronics Company, the world's largest memory chipmaker, in 2002, developed the world's first, two-gigabyte flash memory chip, which can store the equivalent of four movies. The flash memory chip can retain power even if the power is cut off.

Microsoft is developing a multi-use card on which consumers can download their own application software, which possibly means information can be consolidated on to one card (Hansen 2001) enabling readily accessible information available to a person at any time.

Smart cards are invading every aspect of daily life, including public transport of which a $500 million tender was won by Keane Incorporation recently (Ferguson 2005). Haberfield (2005) reported that "smart cards, capable of storing a mass of personal

information including medical and welfare details, could replace Medicare cards from 2006, though no official announcement was made with respect to the commencement date" (p. 22). On 13 May 2006 on Good Morning Australia it was announced that to reduce welfare fraud, identity cards would be used on a "voluntary" basis to claim welfare.

The chip in a mobile phone is being used as a medium of exchange whereby consumers can buy products such as cans of drink, which are debited to their phone account. Telstra and Coca Cola are testing new vending machines which allow customers to "use their mobiles to a dial a number displayed on the vending machine and a charge of $2.20 for the drink, plus a call cost of 0.33 cents, is automatically debited to the customer account Chris Field (Haberfield 2003, p. 9), "What we are seeing is mobiles becoming de facto" (Haberfield 2003, p. 9). According to Consumer Law centre executive director credit cards".

1.3.5 Electronic cash

The company, Keyware, has worked with Proton World to create a biometric e-purse which is a smart card secured by a fingerprint (Dubois 2001), because a "person's unique characteristic" can be identified (Young 2003, p. 69). Telstra has also developed a smartcard to "replace coins at vending machines" (Black 2003, p.21).

Cashless options are expanding, fuelled by improving infrastructure and changing commercial demands. Examples include digital cheques and digital cash which enable many small scale purchases over the Internet to be conducted without the costs inherent

in the credit card networks. An example of the micro payment system is the pay-by-view online newspaper and reference system which uses digital cash that is a completely intangible software-based payment system. The system uses a unique "digital 'coin' which contains information including a serial number, expiration date, the name of the issuing institution and the value represented" (Bollen 2001, p. 7). The digital cash "can be redeemed at a bank for cash or the equivalent credit to an account" (Bollen 2001, p. 7).

E-cash systems are evolving such as Proton used by thirty percent of Belgium's population and Moneo used by ten percent of the population in France (Matlack et al 2002). Bankers and merchants are eager to cut down on the labour and expense of processing small transactions made with cheques and bank debit cards "It's the future: everyone will soon use it" (Matlack et al 2002, p. 4)".

> "…E-money has taken the form of (1) electronic bank notes, such as the embedded chip card known as Mondex or ecash for transfer open computer networks; (2) an electronic check (the researSIC), for transfer over the open computer networks; and (3) enhancements to credit card communications…". (McAndrews 1999, p. 349)

Electronic bank notes, electronic cheque and enhancements to credit card communications can be collectively referred to as digital cash and are designed for electronic transfer over the Internet making use of the network to transmit the necessary information. The electronic bank note contains embedded chips referred to as a "smart card" (McAndrews 1999, p.350) and it is designed as an adjunct to transfer value over the Internet.

Electronic cheques come in various forms but require special details including account numbers which need to be entered on to an Internet site which fulfils the payment requirements. CyberSource offers four electronic cheque options, "CheckFree", "TeleCheck", "AmeriNet" and "Paymentech" (http://www.cybersource.com/products_and_services/electronic_payments/electronic_check_processing/, accessed on 20th December 2006), each with variations of the transfer theme. Credit card enhancements include features using the "smart chip" which allows information to be stored such as enabling special offers and reward points. An example of the enhancements is the American Express card which has been strongly marketing the "smart chip" offering benefits at the point of purchase including chip stored information about retail discounts, special offers and reward points. American Express advertises that the smart chip also has the capacity for additional applications to be added as they are developed and released over time.

1.3.6 Summary

The existing forms of electronic payment, such as EFTPOS and creditcards, continue to replace coins and notes. Many types of cashless mediums of exchange have been developed to improve convenience, save time, increase security and allow entry into the global market. In Australia, Wahlert (1996) has observed the relentless advance of electronic payments has already made us a community with "less cash" (p.8). Many believe that a complete switch to electronic delivery modes is a fait accompli. For large financial payments this is because of their relative safety and speed (Matlack et al 2002, p.1-2).

1.4 Problems of cashless mediums of exchange

With the advantages of convenience and speed of developing money, there also comes a variety of issues.

> "The rapid growth of electronic commerce has been accompanied by an increased number of fraudulent acts facilitated by the unregulated nature of the medium" (Baker 2002, p. 1).

Electronic movement of money has reportedly stripped Russia of much wealth by massive transfer of funds to offshoots of legitimate banks in America. Friedman (2000) quoted by Fossen, (2003) recorded that:

> "of all Pacific tax havens, Nauru has been the most closely associated with the largest money laundering case in world history, the Bank of New York's so-called "Russiagate" scandal" (p. 244).

Fossen (2003) also contributed when talking about the Bank of New York that:

> "Law enforcement agencies contended that the bank case involved at least 87,000 electronic transfers of up to $15 billion (some for capital flight, some for tax evasion, but also some from criminal activities such as contract murder, narcotics trafficking, and prostitution)" (p. 244).

Fossen (2003) used various sources in examining this case including Banks and Exchanges Weekly, Moscow Times, Prime Tass, and Segodnya. From these sources, Fossen (2003) recorded that:

> "Victor Melnikov, deputy chairman of the Russian Central Bank, had stated that $70 billion had been transferred to Nauru from Russia in 1998, compared to total Russian exports of $74 billion. In March 1999, Alexander Pochinok, head of the Russian Finance Department, also claimed that 90 percent of Russian banks maintained 6,600 offshore banking accounts in Nauru, which was receiving $10 billion of Russian flight capital each month" (p. 245).

Tracing the flow of money via a system requiring unique identification would contribute to the solution of these problems. The issue of "crime, fraud and deceit on the Internet" is taken up by Baker (2002) who also examines "a new type of abusive social behavior" (p. 1). Baker examines misuse such as hacking, extortion and perpetrating fraudulent securities schemes. Carding cash or ringing up fraudulent charges to a merchant's account has become easier through the Internet. Baker notes that there is an "emerging electronic black market for stolen credit card numbers" (p. 8).

When trading using cashless mediums of exchange, record keeping functionally replaces cash. Encryption software used as protection is continually challenged by criminals who are trying to break the code. Consequently encryption software needs to be continually updated or else they may not be useful. Legislation has been reviewed but does not seem to be sufficient to protect privacy issues related to cashless mediums of exchange (Young 2003, p. 1).

Other commentators such as Everett-Green (1996), Agre and Rotenberg (1997) and Whittaker (1999) warn of the dangers to privacy, recognising that the more transactions are conducted in cyberspace the easier it becomes to track spending habits, private interests and political beliefs. This is despite the fact that cashless forms of trading such as Internet banking, are highly regulated by Australian finance legislation including specific legislation which deals with electronic payment mechanisms. There are also numerous industry-based codes of conduct including the Electronic Funds Transfer Code of Conduct and the Code of Banking Practice (The Banking Code).

1.5 Verification mark

As discussed this research examines a cashless monetary system involving a portable scanning device, an implanted chip that can be accessed by global positioning satellites that can make use of sophisticated computers for recording fund movements. This system is considered a logical extension of current cashless systems. The system under examination makes use of technologies currently available and affecting work environments locally and internationally but which are not currently used collectively for the application considered by this research. Current applications of the microchip specifically will be examined in this section to show that they are currently available and being used in a range of applications which make it likely that they could be used in the monetary system described.

In Australia the Sydney Swans, an Australian Football League club, are using “computer chips relaying player stress readings directly to coach’s box and a stadium scoreboard”

(Phillips, S. 2004, p.21). Xerox plan to monitor staff movements using satellite technology. Australian Services Union NSW branch president Sally McManus commented that the plan was considered an issue of trust and another layer of monitoring, or surveillance that they are not prepared to bear. The Xerox workers were prepared to 'strike over spying' (2004).

In international applications, a microchip has been inserted under the skin of an arm of Mexico's Attorney-General Rafael Macedo in order "to give him access to a new crime database and enable him to be traced if he is ever abducted" (http://www.wired.com /science/discoveries/news/2004/07/64194, accessed 20th Dec 2006). Some of the Attorney-General's staff have also been fitted with microchips, which give them exclusive and secure access to a national, computerised database for crime investigators. The chips enable the wearer to be found anywhere inside Mexico with the emphasis on the event of an assault or kidnapping. According to Mr. Macedo in the article 'Mexican officials get chipped' (2004), "it's an area of high security; it's necessary that we have access to this, through a chip, which, what's more, is unremoveable," (http://www.wired .com/science/discoveries/news/2004/07/64194, accessed 20 Dec 2006).

A further example of international applications of traceable microchips occurred in Britain where "paedophiles will be tracked by satellite under a new government scheme", "if they go near playgrounds or schools, alarms will sound" (Mancey 2004, p. 34).

Implantable chips are being used in hospitals as identification devices by America's Food and Drug Administration as evidenced by Phillips, G. (2004) who noted that:

> "By implanting microchips in their patients, doctors and nurses will be able to immediately identify the patient just by running a scanner over them. And at the same time they'll receive readout of the person's recent medical history" (p.21).

> "Sufferers of Alzheimer's disease who can't remember their names" "could be scanned and identified easily if found wandering" (p.21).
> "And the chips might also be useful for people suffering cancer, who often have to go through quite complex chemotherapy and other treatment regimes. A chip under the skin should make it easier to keep track of their various medicines and procedures, making mix-ups less likely" (p.21).

Implantable chips can be used as a control feature as evidenced by Applied Digital Solutions , "the US company that makes the implants is hoping gun owners will go for an insert in the hand. That way personalised smart guns could be developed" (Phillips, G. 2004, p.21). Weapons that would only fire if the gun's owner was the one pulling the trigger could be an example. The system would work via a scanner in the gun interrogating the chip in the shooter's hand. If the gun finds the wrong person is holding it, it simply does not fire. Police officers and security guards could be fitted with the system. That way, no one could steal their weapons and use them against them.

Patrons of particular bars in Amsterdam, Barcelona, Scotland and Spain have the option of getting a chip implant allowing them to enter the clubs unimpeded, "they just walked past a scanner at the entrance and straight to the bar" (Beer with microchip 2005, p. 7) no longer queuing to get into the club. The chip also allows management to keep a running total of their tab, "the bartender simply scans their chip and the drinks are automatically added to the bill" (p. 7).

A school in Japan has recently introduced a wearable, rather than implantable, version of the chip (Philips, G. 2004, p.21). These allow the teachers to keep a better eye on the children and determine who is and who is not at school. Legoland in Denmark has wearable chips too. They say they are to prevent kids getting lost.

Evidence has been provided to show that the requisite features of the microchips for the facilitation of the cashless monetary system described currently exist. The features include that it is able to be implanted successfully into humans, it can be used as an identification device that can store and exchange information in real time and via satellite communications. As the system is a recording device rather than an exchange in itself, various credit and debit applications can easily be managed if authorised.

1.6 Benefits of a verification mark

The microchips currently available have high-speed reaction time and can deal with multi-purpose recording functions. If the chip were the culmination of a cashless economy, accounting for personal transactions would become easier including budgets and taxation, which may well be done centrally given all expenditure and receipts would be stored. Non-financial information would additionally be stored which would make personal management of more than just finances possible. The tracking of payments to final consumers would allow a sophisticated audit trail reducing the possibility for fraud. There would also be a convenience factor since a microchip would have plenty of room for other kinds of data (Ramesh, 1997). Cash or credit cards would no longer need

to be carried, and information such as driver's licence and contact details could be stored.

The current benefits of the implantable microchips that were evidenced in the section above include the ability to track people if they are abducted or if they are under a surveillance order such as sex offenders, are prisoners or parolees or for the tracking of young children, people with physical disabilities or those with mental illnesses such as Alzheimer's disease (Crews 2002, p. 2). The implantable microchips can currently provide medical information and increase safety features of weapons.

For national security issues, Defence Minister Robert Hill and Immigration Minister Amanda Vanstone acknowledged an ID card (like microchips) would have to include a biometric element, such as fingerprinting, to be of any real benefit and only if a card could be developed that was not too intrusive (Conway, 2005).

1.7 Hazards of a verification mark

Many of the features that have been described as advantages can also be seen as disadvantages, for example, the ability that allows tracking, increased information and safety features could also enable control.

The storage of records electronically requires very little space. Whilst this record keeping is handled ethically and vast decentralisation of the record keeping exists, privacy can be partially maintained. A perception may arise that the verification mark

would make confidential information about private and business financial affairs vulnerable. Issues of privacy are identified by Phillips (2004, p.21) who states that the problem with an implantable chip is that "you are effectively walking around with a permanent ID tag on you. Anyone with a scanner could point it at you and identify you" (p.21). He is also concerned about information being used as a marketing identification tool.

The more sophisticated the system of collection and the resultant information, the greater the potential for information and, therefore, power asymmetry. Such sophisticated information has the potential also to be misused either by an authority or by unauthorised access, for instance, hackers. A perception may exist that a verification mark would increase the control that regulators, banks or other institutions, have over one's life.

The recent spate of computer viruses (Markoff 2006, p.1-2) indicates the nature of the potential problems that can occur with computer systems. If a cashless medium of exchange reliant on computerised storage global positioning satellites and implantable chips comes to fruition, corruption to the system could have a catastrophic effect.

1.8 Theory introduction

Davis (1989) explored user acceptance of computer technology in business, making use of Fishbein and Ajzen's (1975) and Ajzen and Fishbein's (1980) Theory of Reasoned Action (TRA) as it was "an especially well-researched intention model that has proven

successful in predicting and explaining behavior across a wide variety of domains" Davis et al (1989, p. 983).

The Theory of Reasoned Action was, "born largely out of frustration with traditional attitude-behavior research, much of which found weak correlations between attitude measures and performance of volitional behaviors" (Hale et al 2003, p. 259). In general, the Theory of Reasoned Action aims to contribute to determining the likelihood that a person will undertake a specified behaviour.

The theory "proposes that behavioral intention is a function of both attitudes toward a behavior and subjective norms toward that behavior" (Miller 2005, p.127). By measuring a person's attitudes and subjective norms towards a specific behaviour, which affect a person's intention, the person's actual behaviour could be predicted. Subjective norms are refered to as:

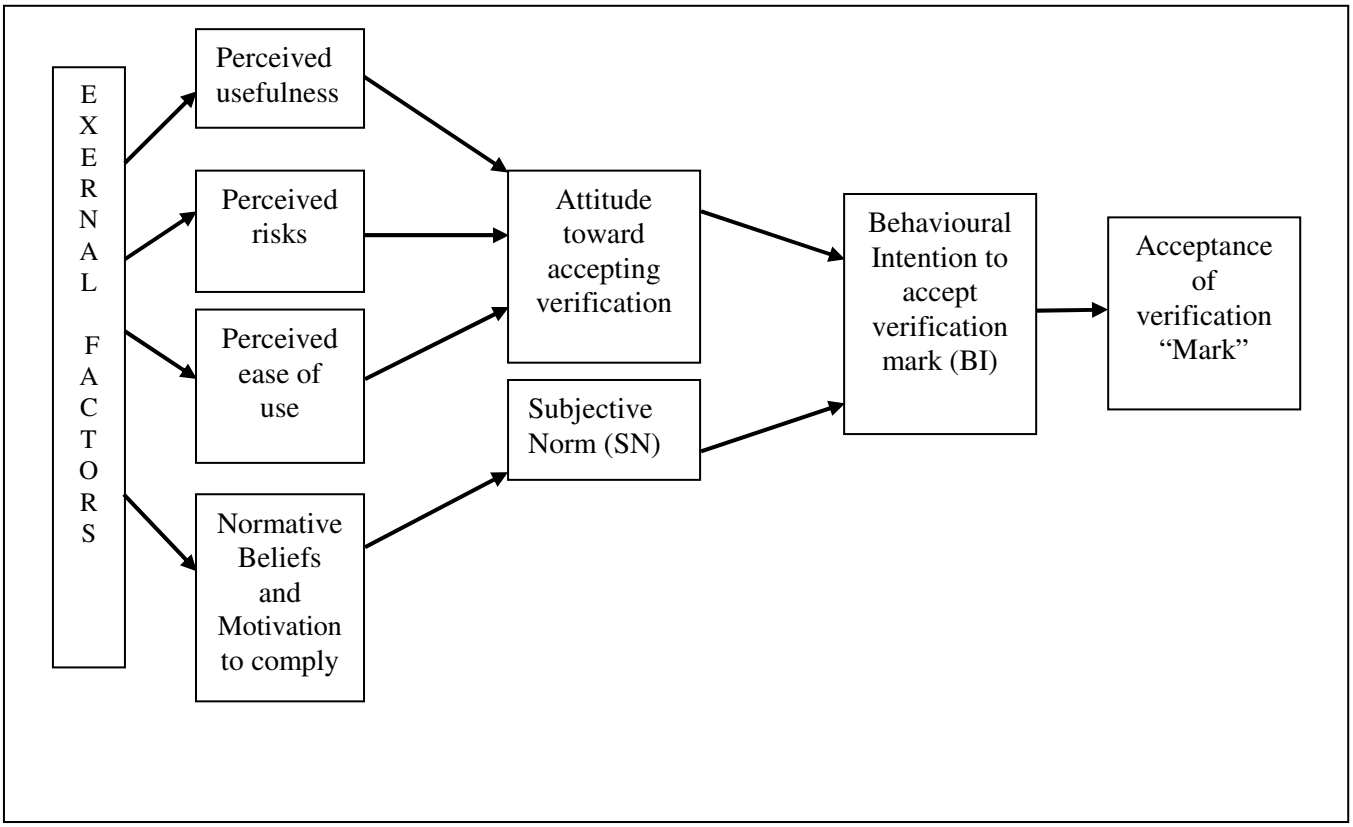
> "the influence of people in one's social environment on his/her behavioral intentions; the beliefs of people, weighted by the importance one attributes to each of their opinions, will influence one's behavioral intention" (Miller 2005, p. 127).

Davis (1989) adapted the Theory of Reasoned Action model to tailor the model specifically for user acceptance of information systems, which he called the Technology Acceptance Model (TAM). Davis posits that two particular beliefs are of primary importance for technology acceptance behaviour. These are the perceived usefulness of the technology for the intended tasks and the perceived ease of use of the technology, which Davis (1989, p. 320) describes as "the degree to which a person believes that

using a particular system would be free of effort". Davis removes the subjective norm from the model completely due to the difficulty "to disentangle direct effects of subjective norms on behaviour intention from indirect effects via attitudes towards behaviour" (Davis 1989, p. 983).

This research disagrees with Davis on the issue of subjective norm and returns to the precepts of the Theory of Reasoned Action model and includes the component before making use of Davis' TAM. A perception of risk is also included as it is seen as important in such a significant and personal decision from a cost benefit perspective. The modified model is designed to apply to the issue of society's acceptance of a verification mark.

Chart 1.1 Modified Technology Acceptance Model



1.9 Research question

The research question of this research asks: What level of acceptance would professional accountants have in adopting a cashless monetary system using an implantable chip technology supported by global positioning satellite and large computer systems? The level of acceptance is considered to be refined by the Modified Technology Acceptance Model which specified four elements that have an effect on the acceptance behaviour of a verification mark. The four elements are perceived usefulness, perceived risks, perceived ease of use, and normative beliefs and motivation to comply.

1.10 Method of Thesis

The lack of research in this area drove the research method towards a broad-based mail questionnaire, reaching greater numbers than would be possible in interviews, focus groups or case-study styles of research. Full members of CPA in Australia and the Institute of Chartered Accountants in Australia were deemed to have appropriate qualifications to address this issue and were selected as the population for this research.

The survey included a series of questions (both open-ended and closed) with the closed questions using a Likert-scale response with a scale between one and five. The survey tested for consistency by using techniques such as asking similar questions in the negative form and found no conflict in the communications of the respondents. The survey was divided into distinct groups including descriptive information, responses relating to the model, acceptance and respondent's belief about the status of existing

technology that would allow the mechanics of a monetary system revolving around an implantable chip. Pre-testing was undertaken to minimise response bias.

1.11 Structure of Thesis

This thesis consists of seven chapters. The introduction provides an overall insight of the research which is followed by the literature review in Chapter 2. This chapter explores cashless mediums of exchange both from a traditionalist and critical perspective of accounting. The chapter traces the development and proliferation of cashless mediums of exchange and new methods of identifications especially the implantable chip as well as their advantages and disadvantages.

Chapter three reviews the various relevant theories including diffusion theory, theory of reasoned action, theory of planned behaviour, and technology acceptance theory. The review led to the methodology used in this research being the Modified Technology Acceptance Model. The four independent variables established from the model (perceived ease of use, perceived usefulness, perceived risks, and normative beliefs and motivation to comply) were then described in chapter four. The research question and hypotheses were also developed and discussed in chapter four.

Chapter five focused on the research method and questionnaire design. Chapter six provides analysis of the responses and the acceptance of the “mark”. The descriptive results were presented and the responses was analysed based on each of the four independent variables. The chapter discussed the availability of technology and analyses

was undertaken on the validity of the research. Early and late response bias were examined and the hypotheses were tested. Further, the chapter examined the responses of open questions in the context of the model. Chapter seven forms the conclusion of the research, provides recommendations and suggests relevant further research.

Chapter Two: Literature review of mediums of exchange

2.1 Traditionalist perspective

Broadly, this research focuses on how financial information affects individuals including their rights. More specifically, the research relates to the acceptance by accountants of a new monetary system based on an implanted microchip (verification mark) as part of a fully automated cashless system which will change how information is gathered, what information is gathered and how that information will be used. The research relates to individual's finances and not the effect on businesses of the verification mark.

If every monetary transaction in which an individual is involved requires transfers using an individual's verification mark, authorisation and a scanner then the amount of centralised data collected would be extremely complete both in amount and coordination. The verification mark would be an implanted chip either in the wrist or forehead. This would contain an individual's record of wealth and personal details. Centralised accumulation of transactions would be automatically up-dated in the same way that a supermarket using a perpetual system and computerised bar-coding scanners can deal with levels of stock. Just as stock purchases increase stock, receipts increase bank balances and just like sales of stock reduce stock levels, payments would decrease bank amounts.

Rights of access to a person's centrally produced records would be available. Individuals and businesses alike would have detailed transaction reports which would cross-reference each other. Primary reports would look like bank statement records or credit card reports.

Electronic information can easily be translated into accounting and taxation reports and, in fact, as all information is contained by central computers an ongoing record of taxation obligations and, therefore, deductions would be available. Scanners would be carried by individuals in convenient locations such as in their mobile phone. This system would stop data being manipulated before, during, or after it has been entered into the information system (Metrejean, Smith and Elam 2004, p. 11-12).

Accountants are interested in financial information in the fulfilment of their traditional pursuits such as completing taxation returns, auditing and preparing financial information and reports. They have the regulatory, professional and individual's permission to undertake these and other related tasks on behalf of clients. For instance, in order to be accredited as a tax agent a person must be qualified under Section 156 of the Income Tax Assessment Act 1936 which requires them to be a member of one of the two premier accounting bodies in Australia and have "successfully completed a course of study in basic accounting principles" (Income Tax Assessment Act 1936, s 156(1)(d)(ii)).

Section 1280 of the Corporations Act requires auditors to hold "a degree, diploma or certificate from a prescribed university or another prescribed institution in Australia" (Corporations Act 2001, s. 1280 (2A)(a)) embracing "accountancy (including auditing)

of not less than 3 years duration" (Corporations Act 2001, s. 1280 (2A)(b)(i)). The Act also requires auditors to be a "Registered company auditor" with the Australian Securities and Investments Commission (ASIC) to audit publicly listed companies. Once again only accountants can act in this capacity for large corporations.

Relevant extensions to their traditional pursuits are also of interest whether that is an anticipated taxation system, a technological change which affects the collection and manipulation of data or the extension of information surrounding financial information. A verification chip would increase the amount and type of information that is currently available on a person's spending behaviour. This trend has been developing as cashless forms of funds have required the support of information trails. Computerisation has made the storage of this information easier and more transferable. One only needs to look at an average credit card statement as evidence of the details available on spending habits that are currently available.

Accountants should be interested in this emerging financial issue as their traditional roles will be affected by it. Accountants have a delegated right to examine sensitive individual information. The preparation of taxation returns on behalf of individuals is an example. With the introduction of a verification mark, taxation accountants will be affected by government regulations on how the information will be collected and how taxation is charged. The hiding of assessable income will take on different forms with the facilitation of the verification mark which will undoubtedly affect the extent and working of the black-market and bartering systems.

Another example of accountants' rights to be involved in personal information is the financial advisor's preparation of a Financial Statement of Advice on behalf of a client. The extent of information that could become available with the adoption of a verification mark would significantly alter how a Statement of Advice is prepared and the extent of that advice. The information available with a verification mark could affect the budgeting of an individual's personal finances which relates not only to financial advice.

From a traditionalist perspective, then, if the verification chip supports collecting increased information then accountants should be interested in the type of information that will be collected and how the information will be used. In accountants' traditional endeavours such as collecting, reporting and managing transactions, they have a delegated right to deal in clients' financial information, from its collection to its use and dissemination. The verification mark will have the potential to alter drastically how financial information is dealt with and accountants' views reflecting the financially literate are important.

There is a plethora of evidence to show that people are concerned with the issues arising from new forms of cashless mediums of exchange. According to Gartner (NYSE:IT) and Jupiter Research in the context of the United States population at the 300 million mark, "80 million consumers who use the Internet do not buy online" and on the other hand, the majority of the online shoppers are concerned about safety and security issues (http://www.technewsworld.com/story/53866.html, accessed on 23rd November 2006).

In making cashless payments removed from the individual, identity is paramount and in the digital era it is embodied in information rather than flesh as evidenced by 'spoofing' (http://www.caslon.com.au/idtheftprofile.htm, accessed on 12th January 2006) or 'joe jobs' (http://www.caslon.com.au/idtheftprofile.htm, accessed on 12th January 2006) where emails or websites purport to emanate from a public figure or private individual in an effort to perpetrate frauds. The Australian Bankers' Association's Code of Banking Practice states that "A Bank may require a customer to notify the Bank as soon as possible of the loss, theft or misuse of his or her payment instruments by unauthorised access by others" (http://www.bankers.asn.au/Default.aspx?ArticleID=95, accessed on 12th January 2006).

In conclusion, accountants have a traditional interest in the development of a cashless monetary system based on implantable chips and real time transactions. Accountants have expertise that would be useful in the context of the monetary system.

2.2 Accounting's role in social development

In the previous section it was argued that a traditional view of accounting entitles accounting researchers to examine issues that may impact upon traditional boundaries such as the sophisticated cashless monetary system using implantable chips. This section argues that other accounting perspectives would also embrace such research as important and legitimate.

The various elements of accounting to many traditionalists are just part of a sophisticated system of collection. They are seen as merely an extension of their historical double-entry origins. To others, like Littleton (1953), when discussing income in the context of it being a force as part of a measurement relationship between input and output and in contemplation that, "income itself confers social benefits" (p. 21), states that in "a large sense, the relations are like those of chemical processes of life itself" (p. 21).

Critical theorists would not want to abrogate responsibility for an evolving accounting process to an authority without input and a full examination of the issues at a macro level and the implications at a micro level. The emerging monetary system discussed in this research would redefine collection and audit processes and deserves investigation prior to its support or introduction even at a voluntary level. Critical theorist literature would be concerned about the method that information is collected, the type of information collected and the use of the information in this emerging cashless monetary system.

Francis (1990) has drawn attention to the way in which critical theorists consider that accounting and the accounting profession have escaped social responsibility. Examples given include its role in the depreciation of the natural environment, and its collusion in denying the legitimacy of the interests of stakeholders other than shareholders. Funnell (1998) contends that the "tendency for accounting researchers is to have been so preoccupied with the processes that form the accounting function that they have overlooked its extended consequences, which do not fall within the quantifiable net" (p. 439). He argues that the link is rarely made between "broader social consequences and

the role of accounting as a constituent element in engendering existing social and political arrangements" (p. 439). Hopper et al (1991) warns accounting researchers not to ignore the "wider social and political collectives" (p. 5). Francis (1990) adds accounting "can influence the lived experience of others" (p. 7). Funnell (2001) even challenges the lack of encapsulation of ethical utilitarian principles stating that it has "contributed little to the interpretation of justice based upon need" (p. 191), in his study of the role of accounting in the Irish famine. Funnell (2001) argues, still referring to the Irish famine, that "accounting played an essential role in confirming the conditions under which property entitlements were determined to be just and in providing apparatus for the State to laager these entitlements" (p. 189). It is, therefore, argued that consideration should be made of the implementation of the verification mark. The way information is gathered, the amount and type of information collected in this system may place an unfair burden on the individuals in the community. The real time collection method also may be considered to be too invasive as it places people at a certain spot at a certain time. The sophistication of the collection system detailed may be seen as unjust.

A system put in place by an authority like a government or businesses like banks extends a sense of legitimacy to it. Many psychological aspects underpin the acceptance decision of a system implemented in such a way. The needs of the community are inferred as more important than the needs of an individual. An individual who does not support the system may be labelled a recalcitrant, unable to deal with change or stubborn. The financial, physical and emotional cost of fighting an established authority where such an asymmetry of power exists, leads to a feeling of being defeated, apathy and preparedness to accept the system even if you do not want to or have doubts. The

social and ethical issues are difficult to argue once a system is in place as you may be labelled as weird.

Hilberg (1985) dramatically argues the Holocaust would not have been possible without the cooperation of the German civil bureaucracy. In this context Funnell (1998) outlines the role of accounting as a component of bureaucratic practices used in the preparation of the Jewish Holocaust. He further highlights accounting as an "ethical practice and therefore having a moral character" (p. 439). Perhaps a pre-acceptance of this may have assisted in diverting the tragedy. If accounting has such responsibility it stands as a justification of research into accounting's roles in future significant projects such as the introduction of a personal verification mark.

Hilberg (1985) contends that "every stratum of society was represented in the envelopment of the victims" (p. 3) of the Jewish Holocaust. Rosenberg (1983) has referred to the bureaucrats as "desk killers" (p. 17) referring to their role in the "labyrinth of bureaucratic routines and apparatus" (p. 17) which contributed to the mass Jewish deaths. "Morality came to be seen as synonymous with discipline and subjugation of all the inner measures of right and wrong" (p. 17).

In this light it seems appropriate to examine whether the verification mark is good in itself and what good might be achieved by its implementation added to the context of a biblical warning against the adoption of "the mark".

The issue of identification and numbering people arose in this Jewish Holocaust tragedy because many Jewish people were indistinguishable based on physiognomy alone. At

one time Jews where forced to wear a Star of David on themselves or their clothing. Identification numbers where also given to the Jews. Some had numbers and/or the Star of David tattooed on their bodies including the back of their heads raising personal rights issues. The numbering system imposed on their bodies was seen to have dehumanised them. An identity number implanted into one's body could also be seen as dehumanising.

Despite the reader's opinions on the views presented in this critical perspective section an argument has been made that justifies further examining the issue of a cashless society based on an implantable chip and associated technology.

The past two sections have represented different accounting positions both traditional and the critical perspective with respect to this cashless monetary issue. Both lead to the conclusion that it is important to examine issues involving the adoption of a verification mark given its potential to affect decision making and accounting systems due to the comprehensive way that information could be collected.

2.3 Proliferation of cashless mediums of exchange

The system of exchange has a history of becoming more sophisticated and in Chapter 1, the development of mediums of exchange was documented. Originally, barter systems moved to physical forms of exchange which eventually led to cash. Systems supporting the value attributed to cash such as cheques and money orders still survive but more

sophisticated debit and credit card systems are common now and allow payment over the phone or Internet in addition to the mail option.

There is evidence to suggest that cashless mediums of exchange are becoming more prolific. There are many applications of cashless mediums of exchange. Cheques, money orders and electronic transfers developed to facilitate payment for goods and services without the need to be present physically. Other associated products establish a store of value such as vouchers and reward points earned from loyalty programs. Debit and credit cards more recently have become normal mediums of exchange. Following on from the physical use of credit and debit cards, bills can now be simply paid by phone or via the Internet by the average consumer. The Internet allows connected computers with protocols that allow interface with different operating software and different applications. "Although a system of networked computers is not new, the recent growth in the significance and use of Internet banking has been astounding" Bollen (2001 p. 5).

Moines (2000) reported that approximately 73% of payments made in the United States are made electronically. The Development Bank of Singapore's debit smart card "money smart" is accepted globally at over 17 million Mastercard locations and can be used to withdraw cash at over 485,000 Mastercard/Cirrus automated teller machines (Ling 2001). The card is highly accessible and can require as little as $100 as a deposit.

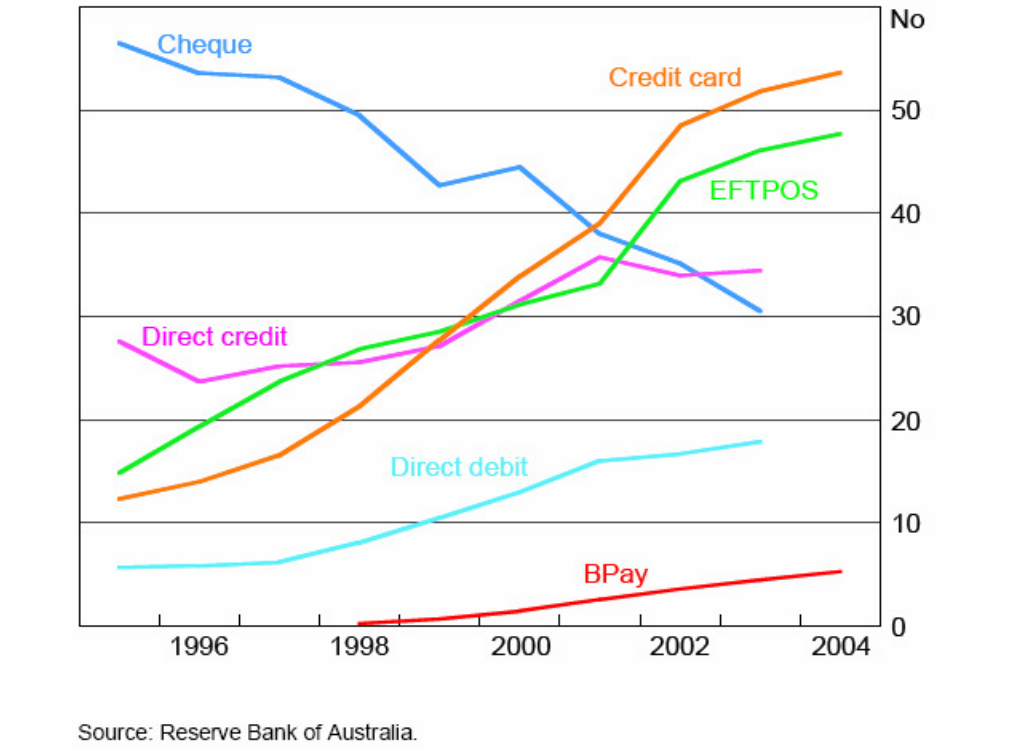
Thirty percent of Belgium's ten million citizens use an e-cash program called Proton for purchases expected to total some five hundred million dollars annually (Matlack et al 2002). E-cash is a prepaid store of cash that can be used at participating vendors via

special readers. In France, the e-card called Moneo has been adopted by ten percent of the people in the regions where it has been introduced. The Moneo e-cash option has been offered to customers on the same card as their credit and debit card (Matlack et al 2002). Moneo is expected to be very successful as the card only costs between five and twelve dollars annually compared with the high fees attached to the debit card system in addition to the propensity of the French to use cheques and money orders.

Harper et al (2005, p. 2) stated that:

> "The technology to support electronic payments, both communications networks and cards, has been available for many years. Credit cards, for example, have been used for more than 50 years. However, the use of electronic payments instruments, especially plastic credit and debit payments cards, has accelerated sharply over the past decade."

Chart 2.1: Non-cash payments per capita (per year) in Australia.



Source: Reserve Bank of Australia.

implanting process

Chart 2.1 shows the "trends towards alternative non-cash payments transactions are pronounced in all developed markets in Australia from 1996 to 2004" (Harper et al 2005, p. 3).

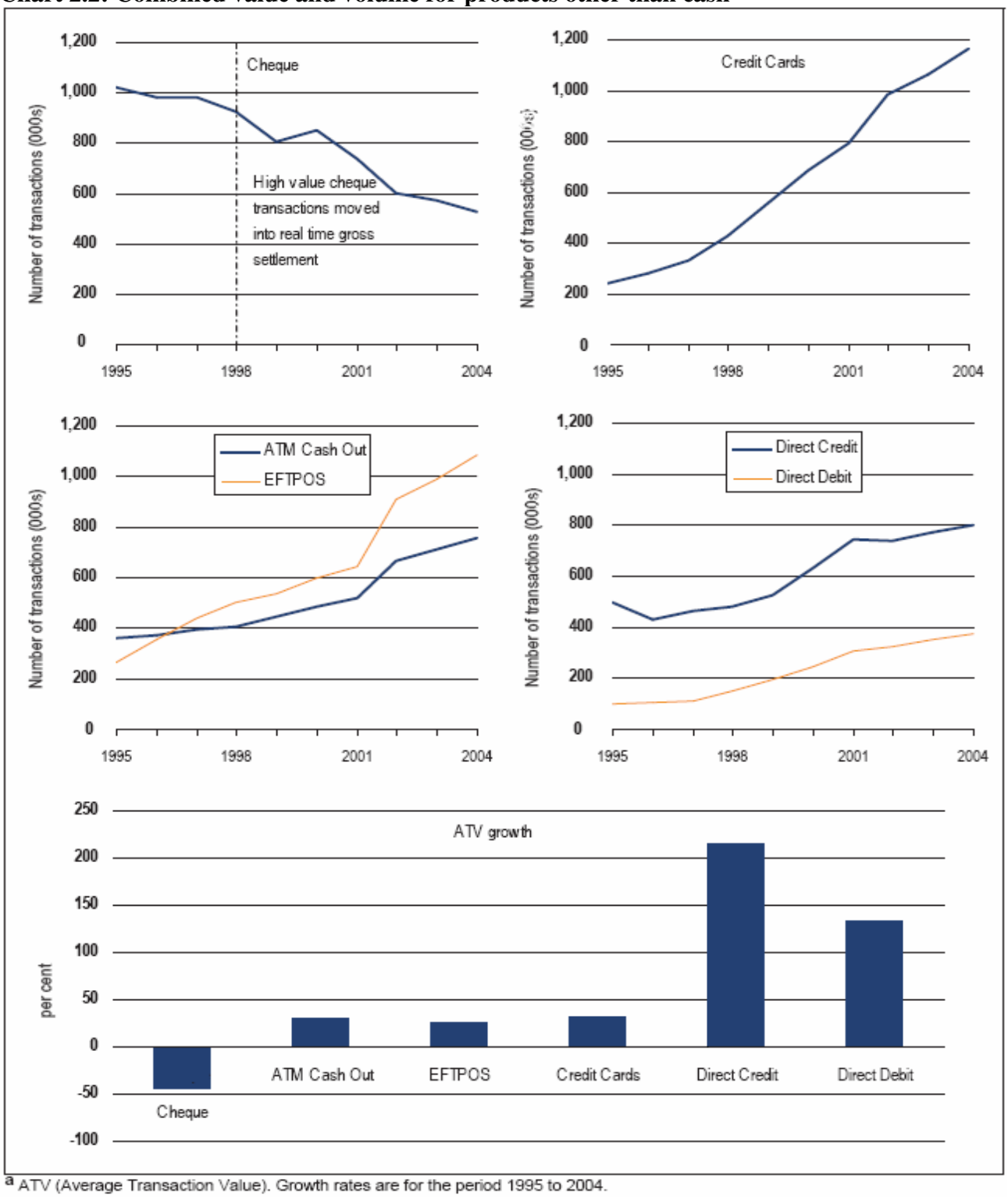
The project team of Exploration of Future Electronic Payments Markets estimates that:

> "in 2004 there were approximately 1.1 billion cash withdrawal transactions in Australia, for an average amount of $160 while the average purchase amount of a cash transaction ranges between $13 and $20" (Exploration of Future Electronic Payments Markets 2006, p. 34).

As electronic payment products become more popular, the total value for cheques has steadily decreased over time. The Chart 2.2 also points out the percentage change of each payment alternatives in Australia from 1995 to 2004 (Commonwealth of Australia 2006, p. 36).

E-commerce overall is an economic powerhouse; "2007 online sales are forecasted at US$291 billion" (http://www.technewsworld.com/story/53866.htm, accessed on 23rd November 2006). In just three years, "alternative payments volume is expected to jump from 12 percent to 26 percent, while credit card volume will drop below 50 percent" (http://www.technewsworld.com/story/53866.html, accessed 23rd November 2006).

Chart 2.2: Combined value and volume for products other than cash[a]



[a] ATV (Average Transaction Value). Growth rates are for the period 1995 to 2004.
Source: Reserve Bank of Australia.

Chart 2.2 evidences the substantial increase in the use of cashless mediums (except for cheque) in both number of transactions and value throughout year 1995 to 2004. Overall, cash transactions "constitute only approximately two percent of the value of all

payments made in Australia". (Exploration of Future Electronic Payments Markets 2006, p. 36).

In 2004, the New Zealand Banks Authority reported that there were "50.8 million 'Internet banking' transactions, and 131.8 million 'PC banking' transactions, illustrating the rapid penetration of these access methods" (http://www.rbnz.govt.nz/finstab/fsreport/fsr_may2005.pdf, accessed on 14th December 2006). It can also be established from this source that there is a trend towards increasing non-cash usage, including credit card usage, arguably because of the convenience of its use. "For example, in the year 2000, New Zealand had 194 million credit card transactions" (Wright 2002, p. 311).

Over the five years reported in Table 2.1, there was an 87% increase in credit card use, from 200 million in 2001 to 375 million in 2005.

Table 2.1: Credit card usage

Year	Credit Card Usage in million	% Change
2001	200	
2002	262.5	31.25%
2003	287.5	9.52%
2004	350	21.74%
2005	375	7.14%

Direct debits have also increased substantially (60%) during the period from 2001 (62.5 million) to 2005 (100 million).

Table 2.2: Direct debits usage

Year	Direct Debits Usage in million	% Change
2001	62.5	
2002	56.25	-10.00%
2003	75	33.33%
2004	81.25	8.33%
2005	100	23.08%

In 2000, "New Zealand had 483 million electronic funds transfer at point of sale (EFTPOS) transactions accounting for around 60 percent of retail sales" (Wright 2002, p. 311). EFTPOS has also been increased dramatically (43.6%) after that as can be seen from Table 2.3, from 487.5 million to 700 million. Further, of all the industries surveyed, the findings indicate that New Zealand organisations are more likely to have EFTPOS (Ratnasingam 2001, p. 7).

Table 2.3: EFTPOS usage

Year	EFTPOS Usage in million	% Change
2001	487.5	
2002	550	12.82%
2003	587.5	6.82%
2004	625	6.38%
2005	700	12.00%

Electronic credits have overall maintained its usage throughout year 2001 to 2005 as indicated in Table 2.4.

Table 2.4: Electronic credits usage

Year	Electronic Credits Usage in million	% Change
2001	312	
2002	300	-3.85%
2003	287	-4.33%
2004	300	4.53%
2005	312	4.00%

Automatic Teller Machine usage has increased at a slower rate (21.4%) from 1.75 million in year 2001 to 2.215 million in year 2005 compared to the non-cash alternatives.

Table 2.5: ATM usage

Year	ATM Usage in million	% Change
2001	1.75	
2002	2.00	14.29%
2003	2.00	0.00%
2004	2.065	3.25%
2005	2.125	2.91%

EFTPOS is widely used and dominates cheques and credit cards (Wright 2002, p. 315). Cheques are less widely used for retail fuel purchases in New Zealand (Wright 2002, p. 313). Cheque usage, the non-cash alternatives without the immediate verification of other non-cash alternatives such as credit card and EFTPOS has been decreasing at a substantial rate (21%) over the five years (2001 to 2005) examined in Table 2.6.

Table 2.6: Cheque usage

Year	Cheque Usage in million	% Change
2001	237.5	
2002	237.5	0.00%
2003	225	-5.26%
2004	200	-11.11%
2005	187.5	-6.25%

2.4 Advantages of cashless mediums of exchange

The various cashless options provide specific advantages to the user. Amongst the most important of these advantages is the convenience of payment. With cashless forms of exchange it is not necessary to carry sufficient cash for purchases, which could be large amounts which, in turn, could be lost or stolen. There is also no need to be physically present to pay a bill which can often be conveniently paid via the mail, over the phone or via the Internet. Credit facilities can also accompany cashless mediums of exchange so purchases and payments can be made without the need to have cash actually available at that time. For example, ANZ Frequent Flyer Credit cards offer up to 55 days of free credit, associating with reward point accumulations which can be used to redeem products or services including airline tickets. The monthly statement is considered an organised documentation of expenditure. This can be an important source of information for the preparation of taxation returns, personal budgets or an analysis of spending. The documentation involved in a credit transaction enables security advantages such as the ability to trace the payment to its source in order to determine its legitimacy; this is not possible in a cash transaction without associated paperwork.

When prepayments are made for a good or a service the manner in which the payment is made when the payee becomes bankrupt or goes into liquidation affects the payer's entitlements. "The cash payer is in the worst position and will become an unsecured creditor whilst other forms of payments such as a cheque, credit cards and possibly electronic payments may allow revocation of payment" (Edwards 2004, p. 81).

"Many firms, particularly those involved in handling large amounts of coinage and bank notes, are finding the costs of handling cash to be increasingly onerous" (Stuber 1996, p. 8). "Cashless mediums of exchange makes a clear way to consolidate and extend such means of reducing the costs of undertaking small-value retail transactions" (Ioannis 2000, p. 8).

> "Consumers would no longer need to have the correct change for a transaction or to handle numerous small coins. The incidence of error in calculating change from a transaction would also be reduced" (Stuber 1996, p. 9).

Finally, "cashless mediums of exchange makes improvements in the efficiency of financial arrangements that reduce or destabilize the demand for the monetary" (Woodford 1998, p. 218). Cashless mediums of exchange "need not be a source of macroeconomic instability" (Woodford 1998, p. 218).

The costs of cash include the risk of handling it including the risk of loss, theft, safekeeping, deposits of currency and security. Recording cash is also costly including the point of sale collection of the transaction details, accounting and dealing with the associated financial institution.

2.5 Disadvantages of cashless mediums of exchange

Godschalk and Krueger (2001, p. 13) outlined the disadvantages of using e-money including the need for hardware, the expenses and "conflicts with anonymity" (p.13) of security and the fact that it is not suitable for hoarding.

With the convenience of cashless mediums of exchange often comes the reality of dealing with lines of finance that are often associated. The success of credit cards and the high establishment fees and interest rates are a testament to people' inability to manage their money and, for many, to spend within their means. That credit is provided does not guarantee that the recipient will be able to manage the repayments and often financial difficulties result.

In the search for greater convenience of exchange new social issues are created. The tracking and generation of information that is created as a function of cashless mediums of exchange create issues such as the control an authority has over an individual. A related issue is the level of privacy afforded to a person by the system and the use that is made of the information by authorities in controlling behaviour and by those who may misuse the information in illegal or immoral ways. As systems of exchange develop, there is a greater dependency on technology, which is also subject to system corruption or failure.

"Digital cash is ideally suited for international money transfers and, aided by computer software, could be routed and re-routed to several destinations internationally within seconds" (Wahlert 1996, p. 24).

> "The advent of cashless payments mechanisms erodes the monopoly position of the central bank as the sole supplier of currency which represents a return to privately-issued currency, something not observed in Australia since the early years of this century" (Grabosky and Smith 1997, p. 3).

> "The proliferation of electronic funds transfer systems has enhanced the risk that such transactions will be intercepted and funds diverted. Existing systems such as ATMs, and EFTPOS technologies have already been the targets of fraudulent activity, while home banking and internet shopping with the use of electronic cash will provide rich new avenues of fraud in the future" (Grabosky and Smith 1997, p. 3).

2.5.1 Cashless mediums of exchange's propensity to magnify an authority's control

The bartering system is predominantly free of social control issues as there is no primary evidence of the exchange other than a good or a service. The time, amount, subject of the exchange and other details are not documented primarily in the exchange. The barter system obviously lacks the sophistication required in a developing society. The nature of cash itself also lends itself to a lower level of concern regarding control. Likewise cash is not typically traced to a particular person even though the notes themselves are individually coded. A secondary system of tracking is required to ascertain how much cash a person receives and spends which has always been an issue in the appropriate

collection of taxation. The lack of information that a regulator has about cash transactions not supported by documentation reduces the potential the government has over the transaction including the collection of relevant taxation, the legality of the good or service. This lack of control over the transaction manifests in a lack of control over the person making the transaction at least from this source and includes an inability to gather information to profile the individual making the transaction.

"Under the table" cash payments to avoid taxation or other regulations are an issue with cash. The New Zealand Warriors organisation had been caught paying undisclosed cash payments in excess of a million dollars to its players during the 2004-2005 season. These transactions had not been recorded as a method to avoid the salary cap restrictions (Warriors ponder appeal to get points back 2006) imposed by the National Rugby League (NRL) who, upon investigation, fined the club $430,000 for salary cap rorting. As cash is typically not traced to a specific person, how a person spends their money can be kept relatively private. Misuses, in the first instance, are contained to the transfer of a physical currency, for example, a robbery or blackmail situation. The government to some extent controls the amount of cash in circulation via monetary policy, but as it is in a physical form and not an electronic form, then it is not dependent on a recording system which could be tampered with or corrupted.

Non-cash transactions often require documentation and often generate an electronic record. Examples include credit card transactions and interest payments made to a customer by a financial institution whereby the client and financial institution have electronic records and the client is sent a paper version at some predetermined time. With a credit card, the vendor, customer and the financial institution have a copy of the

transaction whether in paper or electronic form. When an electronic trail is established, potential access by various bodies including the government or a legal authority is made possible. No longer is the transaction anonymous. For example, it is common taxation audit practice in the Australian Taxation Office to match electronically generated income such as interest that is recorded by a financial institution with an entity's taxation return. If the amount is not disclosed in the entities tax return, this can trigger a more expansive audit or at least an official letter to the taxpayer requiring the income to be included. Another example of an authority's intervention is where amounts are considered fraudulent or illegal and a warrant is obtained allowing the governing body, most often a police squad, access. A police squad may freeze the amounts and examine the electronic trail for evidence of infractions.

The increased knowledge facilitated by the necessary record keeping of most cashless mediums of exchange adds to the asymmetry of power between the individual and the government. The government is in a stronger position with respect to the information available to it than before the recording of such transactions. The fact that an authority can, if it chooses, view a person's transaction history with most cashless mediums of exchange, is analogous to Bentham's concept of a Panopticon (Rabinow 1982). Rabinow (1982) stated that Foucault was intrigued with this concept because of the underlying social issue of control. The Panopticon was a society, built for observation, designed for the eradication of disease. Rules were developed to limit the spread of the disease, for instance, affected parties were not allowed to leave the vicinity. A viewing quarter was established whereby authorities could see out at any time they chose but physical characteristics meant no one could look into the viewing quarter. When referring to the supervisor in the Panopticon, Bentham states the "invisibility is a

guarantee of order" (Foucault 1982, p.200). He warned, "visibility is a trap" (Foucault 1975, p.200) stating that "he is seen but he does not see; he is the object of information never a subject in communication" (Bentham 1791, p. 60). In this analogy cashless payments can be viewed as desired forming a strong system of control. Bentham's panopticon was a control-based system developed for a worthy cause, nevertheless Foucault warns of the social control issue. A cashless society may be viewed similarly.

Broadbent (1995) also examined the issue of visibility when he stated "making certain aspects of reality 'visible' creates the possibility of controlling these elements" (Broadbent 1995, p. 4). He continues that "its control potential which constitutes its real social influence as well as its social danger".

2.5.2 Privacy issues arising from cashless mediums of exchanges

The bartering and cash systems often did not provide the opportunity for privacy to be compromised outside those involved in an exchange. Recording systems are required to make a cash or barter exchange subject to privacy issues. "When trading using cashless mediums of exchange, however, record keeping functionally replaces cash. These ubiquitous records imperil privacy" (Young 2006, p.1). Already much information has been collected about individuals for many reasons including the developing cashless means of exchange. The trend towards increased stored information is continuing. According to Jackson (2003),

> "an important concern about e-commerce shared by consumers has been a fear that their credit card information may be used fraudulently or be disclosed to others who then use them fraudulently" (p. 28).

Despite the legal attention that privacy issues gain, common law has not defined it. "The Victorian Law Reform Commission observes that: the term [privacy] has different meanings in different contexts" (Doyle et al 2003, p. 238). As there is no clearly accepted meaning of the term, privacy, Doyle examines the literature from the narrow to the very broad noting the definition by Warren & Brandeis (1890) which is the "the right to be let alone" (Doyle et al 2003, p. 239) which "has been described as influential for over a century" (Doyle et al 2003, p. 239).

In recent times with the pressure of the information technology age, Gavison's broad definition of privacy stated in Doyle et al (2003) has been useful. Her definition is "limited access in the senses of solitude, secrecy and anonymity" (Doyle et al 2003, p. 239). Gavison views privacy

> "as a measure of the extent to which an individual is known, the extent to which an individual is the subject of attention and the extent to which others are in the physical proximity to an individual. Her definition of privacy was to include …such "typical" invasions of privacy as the collection, storage, and computerisation of information; the dissemination of information about individuals: peeping, following, watching, and photographing individuals intruding or entering private places; eavesdropping, wiretapping, reading of letters, drawing attention to individuals, required testing of individuals; and forced disclosure of information" (Doyle et al 2003, p. 239).

Doyle et al (2003 p. 239) observes that

> "…control of personal information" underlies all the definitions and contributes that the right to privacy amounts to the ability to keep from others information about oneself. There is no scope of this information; it extends to such matters as employment history, current income, political persuasion, religious beliefs, sexual orientation, hair colour, height and one's hopes and fears".

Electronic transfer of exchange over the Internet creates a plethora of privacy issues including the ability of the web server via the cookie features in browser software to identify a web client "and enables certain features that are useful for surfing and online commerce, such as retaining screen preferences, storing passwords, and creating virtual shopping carts" (Riley 1998, p. 89). In addition,

> "it is possible that every Web site visited, every message sent or received, and every purchase made can be recorded in a database available to a wide range of users for a modest fee" (Shapiro 2000, p. 190).

Cashless mediums of exchange add to the records kept about an individual and in potentially highly sensitive areas. The mere consolidated visibility affects a person's privacy whether that information is specifically used or not.

As an example of data collection, Australia Post recently undertook an "Australian Lifestyle Survey" (Australian Post Survey, July 2002). Recipients were asked to complete a form containing questions about personal details and preferences with a promise to ask only relevant "information" (Australian Post Survey, July 2002). A lure

of a $25,000 prize was used to entice participants. The information was assembled as a marketing tool but more clandestine purposes such as selling the information is expected; however, this is not advertised.

Privacy is an increasing social issue. Can the controller of the increased and consolidated personal information be trusted to use it in a manner that the community finds acceptable? Recently, personal information had been collected and sold for profit by an Australian business entrepreneur raising privacy issues (Carroll 2002, p. 48). In July 2000, Toysmart.com, an internet retailer, planned to sell its consumer information database as its most valuable assets after its declaration of bankruptcy sparked the enforcement action by the Federal Trade Commission (FTC) and the company ordered not to sell its consumer database information (Carroll 2002).

In an effort to protect privacy two methods arise: first, the technical protection afforded to a person's information, and second, a person's formal protection.

2.5.2.1 Technical protection of information

On technical protection, the encryption software sourcing from the United States has been of significant technical quality enabling information to be sent across computer networks without fear of tampering. However, technical protection is a moving target as those trying to penetrate the measures become increasingly sophisticated as well.

> "The United States government had curbed the export of these encryption software products via legislation before introducing amended legislation that has ended many restrictions on the export of the products" (Tigre 2002, p. 39).

Business will inevitably pressure legislators to sacrifice security for profit as evidenced by this bipartisan group of technology companies and trade groups who argued that the existing export controls would have put the United States products at a disadvantage in the global market place as demand for computer-security products grew. The United States federal government are now allowing the market to decide the appropriate forms of encryption for electronic data, but what of the interests of the powerless?

2.5.2.2 Formal protection of information

Is legislation sufficient to protect the privacy of the community? The Australia Card proposal in many ways raised the issue of privacy in a public forum in Australia. The referendum to introduce the Australia Card failed. Privacy issues may have been a factor in the cards' rejection. The government subsequently introduced a unique numbered identification system via the Australia Business Number. The Tax File Number is also a unique identification number system used by the government. If these numbers are not quoted when required by law there is significant impact on the taxpayer. In terms of tracking every individual, the Australian Business Number system does allow entity owners to have more than one number that they can use and not all people are required to have a number.

"The right to privacy as such does not exist at common law in Australia. Such legal protection as exists is provided incidentally by other causes of action" (Doyle et al 2003, p. 237). High Court Senior Judge Skoien in ABC v Lenah Game Meats Pty Ltd (2001) 208 CLR 199; 76 ALJR. Dean (2004, p. 114) declared that:

> "there cannot be a civil action for damages on the actionable right of an individual person to privacy. But I see it as a logical and desirable step. In my view there is such an actionable right."

On 16 June 2003 a Queensland district judge in Grosse v Purvis [2003] QDC 151, (Dean 2004, p. 114) declared a preparedness to take up the challenge of the High Court to declare a tort of privacy when the district judge awarded $178,000 in damages with respect to the right of an individual person to privacy. In commentary Dean (2004, p. 114) noted the "Australian legislature's hesitancy" and put pressure on the courts to fill the void left.

The data protection regime in Australia includes the Information Privacy Act 2001 (Vic), the Privacy and Personal Information Protection Act 2000 (NSW) and the Information Act 2002 (NT) along with the Australian Federal Privacy Act 1988 which authorised the implementation of the eleven principles developed by the Organisation for Economic Cooperation and Development in 1980. The eleven principles are as follows:

1 - Manner and purpose of collection of personal information;

2 - Solicitation of personal information from individual concerned;

3 - Solicitation of personal information generally;

4 - Storage and security of personal information;

5 - Information relating to records kept by record-keeper;

6 - Access to records containing personal information;

7 - Alteration of records containing personal information;

8 - Record-keeper to check accuracy etc. of personal information before use;

9 - Personal information to be used only for relevant purposes;

10 - Limits on use of personal information; and

11 - Limits on disclosure of personal information.

Guidelines to the "National Privacy Principles" (Jackson 2003, p.22) were written by the Commissioner which included how information is collected, used and disclosed. The guidelines also consider the data's quality, security and openness along with how the data were accessed and corrected. Data identifiers were considered along with the anonymity of the data, trans-border data flows and how sensitive information was handled.

The Act was extended in December 2000 via the Privacy Amendment (private sector) Act to include most private organizations and set out how organizations should use, keep and disclose personal information. The Privacy Commission has jurisdiction not only over the Privacy Act but also over other related areas such as the entitlement to investigate breaches under Part VIIC of the Crimes Act 1914 and jurisdiction over the Data-Matching Program (Assistance and Tax) Act 1990. The Commissioner also has monitoring and compliance functions under the Telecommunications Act 1997 and responsibilities under the National Health Act (1953).

In deference to the amount of information in the community, the Corporations Act 2001 requires a company to keep a register containing certain personal information such as a shareholder's name, address, the number of shares held, the date of the first purchase of shares and the shareholder's Tax File Number. This information is to be protected and a privacy policy is to be adopted and disclosed. Australian Mutual Provident Society (2002) in its policy states that the information "can only be disclosed to members of the group and other members of the computer share group, your broker, external service supplies, mailing and printing companies, Australia Post, banks, building societies and credit unions, ASX and other regulatory authorities and anyone you authorise".

The Australian Law Reform Commission in 2006 released Issue Paper 31 entitled, Review of Privacy. The paper outlined the privacy regulatory environment in Australia including the Privacy Act 1988 and the Privacy Principles. The project confronts the issue of the impacts of developing technology on privacy. The paper concentrates on the internet and, in particular, on cookies, web bugs, hypertext transfer, protocol and spyware.

The paper also tackles the issue of "Unique Multi-Purpose Identifiers" (http://www.austlii.edu.au/au/other/alrc/publications/issues/31/12.html, accessed on 6th February 2007) and then proposes the "Australian Government Access Card" or "Health and Social Services Access Card" (http://www.austlii.edu.au/au/other/alrc/publications/issues/31/12.html, accessed on 6th February 2007).

The examination of the attempt to protect privacy begs the question; can the government be relied upon to protect privacy? Does the community believe that either legislation or

an amended constitution can always protect their privacy in the way that they desire? In many areas, the lack of resources compromises good protection.

2.5.3 Abuse

Cashless forms of exchange changes the potential related risks. Rather than the physical stealing of goods or cash, more clandestine frauds revolve around the recording and transfer of the exchange. A stolen credit card, a forged signature or a forged transfer of funds are also examples. Various forms of fraud exist online. Phishing is an activity attempting to "fraudulently acquire sensitive information such as usernames, passwords, and credit card details, by masquerading as a trustworthy entity in an electronic communication" (Jakobsson 2007). Trojans is one of the programs that is designed, in the context of computer software, to do various harmful things such as remote access, data destruction, and adding or copying data from infected computers (http://en.wikipedia.org/wiki/Trojan_horse_(computing), accessed on 10th March 2007). In 2005, in the United Kingdom,

> "total losses from online banking fraud reached £23.2 million, an increase of 90% from the previous year's total of £12.2 million. This figure is relatively small when compared with plastic card fraud losses £439 million" (http://www.apacs.org.uk/resources_publications/documents/FraudtheFacts2006.pdf., accessed on 4th December 2006).

In Risk Management for Electronic Banking and Electronic Money Activities prepared by the Basle Committee on Banking Supervision (http://www.bis.org/publ/bcbs35.pdf, accessed on 4th December 2006), "employee theft of smart cards" (p.18) has been

identified as an abuse which may result in possible losses from redeeming electronic money for which no corresponding prepaid funds were received. As a result of this fraud, customers may perceive the bank as being unreliable and the bank may face legal or regulatory sanctions, and negative publicity (http://www.bis.org/publ/bcbs35.pdf, accessed on 4th December 2006).

2.5.4 Technology issues

An examination of the control environment surrounding cashless mediums of exchange raises issues of fraud at a level perhaps not thought of with physical mediums of exchange. The Australian Institute of Chartered Accountants Australia President, Byram Johnston, explained that simple fraud on the Internet involving stolen identities and passwords to encrypted information protection on the Internet "allowed organised crime to do away with banks transferring money across national boundaries" (Johnston 1997, p. 35). It is possible for "an untraceable virtual currency for international criminals to be created on the Internet (Johnston 1997, p. 35).

Computer hackers deploy a Trojan horse into programs that copy passwords when Internet users log on to remote computer systems through the vast network. Estimates of the amount of money lost to taxpayers each year due to fraud in the Commonwealth Government vary wildly. At the low end, the amount has been put at less than $2.5 billion. The Australian Institute of Criminology believes fraud in the public sector is as high as $13.8 billion (AIC 2003 Annual Report Identity Fraud: An evaluation of its nature, cost and extent). As solutions are sought to reduce potential problems in cashless mediums of exchange, a method of identification linked to a numbering system may be

considered as a final verification of the recipients of funds making tracing culprits easier and fraud harder.

The solution to unauthorised use of cashless mediums of exchange may be in the unique identification of individuals via such means as a fingerprint identification solution linked to a numbering system. This may be considered as a final verification of the recipients of funds making tracing culprits easier and fraud harder (Michael et al 2006, p. 12).

2.6 Method of identification

2.6.1 Identification has become a national issue

Identification of individuals is an increasing national issue for reasons including combating terrorism and identity fraud which "cost Australia about 1.1 billion in 2001 and 2002" (Crawford 2005, p. 31). Evidence of the issue is the federal government's integration of "national databases to better identify Australians" (Lapthorne 2005, p. 15). According to Attorney General Phillip Ruddock, "the government was trawling through databases including Medicare and the Australian Taxation Office to cross reference Australian identities partly to prevent identity theft" (p. 15). "With the Blair government contemplating a national ID card system, Mr Howard said he was open to a renewed debate in Australia" (Harvey et al 2005, p. 17).

Fake identification has caused great concern for government agencies who have progressively added security features to identification documents such as holograms, shadow pictures and bar codes; however "the Internet sites that sell fake IDs appear to have kept pace" (Moor 2002, p. 28). Tinkler 2006 (p. 17) reports that realistic fake ID's can be bought for around $25 and that it is so easy to obtain the ID's that photo IDs were obtained for Victorian Premier Steve Bracks, police commissioner Christine Nixon and fugitive drug baron Tony Mokbel which were received within two weeks of ordering them.

Crawford (2005) talks of new supervisory powers which allow a registration database of sex offenders, which "records current and previous names, addresses, car registration and even distinctive birthmarks" (p. 11). The new supervisory powers allow "up to 15 years monitoring possibly by electronic bracelets under the Serious Sex Offenders Monitoring Act 2005, Section 9c.

The Health Minister's acknowledgment that it has tested a system to share patient information has raised concerns about the possibility of an Australian card or national identity card" (Nicholson 2003, p. 2).

Hundreds of murders, rapes, abductions and other serious crimes have been solved using DNA taken from Victorian prisoners. The latest statistic reveals that since June 2000 DNA tests have lead to 922 inmates being charged in connection with 1552 previously unsolved crimes (Haberfield 2004). According to Victorian Police Minister Andre Haermeyer, another 243 cases had been solved after court orders were taken out to force prisoners to give DNA. In more than 600 cases DNA evidence from one crime scene

had been linked to another. DNA matches had been found in the cases of 1300 burglaries, 48 aggravated burglaries and 70 thefts. Victorian Police also used DNA evidence to prosecute prisoners for murder, rape, abduction and assault. Andre Haermeyer said that "DNA evidence is giving criminals nowhere to hide and has been an enormous success story for Victoria police," (Haberfield 2004, p.21). "The Office of Attorney-General Rob Hulls will examine a legal loophole that has allowed police to collect genetic material free from regulation or independent review" (Giles 2004, p. 14). The Ombudsman has warned "the covert police checks are not covered by law" (Giles 2004, p. 14).

Even parents are storing DNA from children as part of an identity kit offered by ChildsafeID which for $25 includes "a fingerprint, DNA swabs kit" (Papadakis et al 2005, p. 30).

Other physical identity controls are also becoming a reality. Wallace (2003) describes a federal government "probe into the use of iris scanning, fingerprinting and other biometric technologies on welfare recipients" (p. 14). This has been 'in response to growing identity fraud problems leading to cheats claiming the dole under up to 33 different names" (p. 14).

2.6.2 Identification is a global issue

The identification issue is not confined to the local environment. In the USA in 2001, bills were passed in Congress to allow for the creation of three new acts related to biometric identification of citizens and aliens, including the Patriot Act, the Aviation and Transport Security Act, and the enhanced Border Security and Visa Entry Act" Michael et al (2005 p. 25). Ten states in the USA continue making use of fingerprint technology, and occasionally, of face recognition technology, to screen individuals for duplicate applications (Bunney 2003, p. 12), which is to prevent people from holding more than one identification.

In South Africa, a biometric solution was found for approving pension payments to an illiterate rural population where claimants verify "their identity by presenting a fingerprint for matching against one previously enrolled to the database" (Bunney 2003, p. 11). "False negatives do occur with fingerprints damaged or eroded by the typical rural way of life" in those circumstances a "verification based on a stored photograph of the claimant" is used.

In Malaysia the national ID card is already in use to support welfare payments (Bunney 2003, p. 13). The Malaysian identity card has convenience factors as it has eight applications being "driver's licence, passports, Touch 'n Go card, health information, e-cash, automated teller machine (ATM) card, and the public infrastructure key" (Pardas 2004, p. 2).

"The Philippines recently began deployment of a Social Security Card system designed to record entitlement and protect welfare and retirement payments" (Bunney 2003, p. 13).

The Straits Times documents that

> "residents in Thailand's Muslim-dominated southern border province of Yala are flocking to the local districts offices to apply for the new 'smart' ID cards, according to local government officials. The demand is so high that the authorities have decided to register applicants until 10pm everyday even on weekends. Thai expatriates living in Malaysia have also shown interest in having their current IDs replaced with the 'smartcards'. The government is introducing the new ID cards throughout the country in stages". (Southern Thais eager for "smart cards", 14 Oct 2004, p.42).

In a joint project between the Malawi government and the United States Federal Reserve Bank a "low-cost memory smart cards storing encrypted fingerprints offers ATM access to cash, point-of-sale payment with PIN or fingerprint, and a fuel payment system" (Bunney 2003, p. 13).

2.6.3 Types of identification solutions

There are various ways of identifying people. The uniqueness of people is a very well used area of identification referred to as biometrics. These vary from fingerprints, retina or iris scans, facial characteristics, keystroke style, voice patterns to DNA.

Biometric input devices usually consist of a device such as a camera or scanner that collects image data. A template is then developed by an algorithm which allows it to be matched.

The fingerprint is the most commonly used authentication biometrics. Bunney (2003, p. 12) confirms the "matching of fingerprints" "technology certainly does work, as police forces worldwide have proven". Fingerprinting makes use of distinctive patterns of skin ridges.

> "The principal types of patterns are arch, tented arch, radial loop, ulnar loop, and whorl. Most fingerprint scanners use technologies that measure the optical, capacitive thermal or ultrasonic characteristics of the fingerprint. Newer devices incorporate solid-state scanners that consist of a piece of silicon containing an array of sensors" (PriceWaterHouseCoopers Risk Management Forecast 2001, p. 206).

The physical identification can provide a sophisticated audit trail of exactly who authorised a particular transaction. Questions, however, are now being raised about how unique a finger print actually is. Tim Robinson from BioPay, one of the largest companies involved in fingerprints at checkouts, believes "it's inevitable that people will use biometrics to initiate financial transactions (Saitz 2003).

De Souza (1997, p. 58) describes an inkless electronic fingerprint reader using credit cards at point-of-sale terminals which uses a "low cost silicon tactile imager for reading embossed characters on credit cards".

Another popular biometric uses the human eye as a unique identifier. The uniqueness of the iris and retina are currently used for authentication. The iris is the "opaque contractile diaphragm around the pupil, which is the coloured part of the eye" (PriceWaterHouseCoopers, Risk Management Forecast 2001, p. 206) which has folds and freckles which are unique. "The retina is the area at the rear of the eyeball on which images are formed" whose "blood vessels form unique patterns" (PriceWaterHouseCoopers, Risk Management Forecast 2001, p. 206).

Recently the technology became available to video images of people's retina as part of a recognition program dismissing the perception that a laser was necessary as part of the recognition process. It was estimated that the majority of banks would use the technology before the year 2008.

Another biometric is hand recognition which is accomplished by "comparing the length, width, thickness and surface of the hand and four fingers. Scanners use a 32,000-pixel charge-coupled device" (PriceWaterHouseCoopers, Risk Management Forecast 2001, p. 206).

The human voice can also be used for authentication purposes as it is affected by the "shape of the throat, larynx, and sinus cavities" PriceWaterHouseCoopers Risk Management Forecast (2001, p. 208) even though it is "not a true biometric" (p. 208) because it can varied at will.

> "The quality of the signal that reaches the central processor can affect the validity of the tool. Microphones can have frequency responses that distort the signal whether they are freestanding or via the telephones which are often noisy" PriceWaterHouseCoopers Risk Management Forecast (2001 p.147).

The Age, a Melbourne newspaper, (5th September 2005, p. 3) reported that one application of voice recognition software is the checking that soccer hooligans are at home during soccer matches via computer generated voice verification software.

Handwriting recognition, also known as "dynamic signature verification, is behavioral and not a true biometric but is often used for recognition purposes" (PriceWaterHouseCoopers Risk Management Forecast 2001 p.147). Typing or keystroke is also behavioural. "Keystroke recognition measures the rhythm of the typing of a key word or phrase" (PriceWaterHouseCoopers, Risk Management Forecast 2001, p. 208). Tiredness, for instance, can affect a person's keystroke making the method unreliable.

2.6.4 Numbering

"Uniqueness is an important element of control" (Young 2003, p.69) as an identifier which needs connection "with a logical numbering system" (Young 2003, p.69). Without direct access to the system, an identification number would have to be remembered and vendors and authorities would need some style of traditional identification such as a card. To facilitate a monetary system, a permanent record would be required so that it will never be forgotten or lost as a means of eliminating fraud and

extortion. People would need to be numbered in a manner similar to the way products are often bar-coded. An application of the success of numbering is Fong's (2006) report that a new database of the identity card numbers of stolen phones has contributed to a 20 percent reduction in mobile thefts in Singapore.

Biometrics can be stored on a smart card to verify that the holder of the card is actually the owner of the card (Dubois 2001) whether this is via voice, face, fingerprint or other feature. Alternatively, a number could be applied to each individual using methods such as the new "black light" tattoos which are "almost invisible in day light but show in great detail in black light" (http://abcnews.go.com/Technology/popup?id=2339802, accessed on 6th February 2007). Black light is a reference to ultraviolet light. The laser painlessly destroys the pigment of the skin but it is so extremely fine, that it is invisible to the eye. (http://www.wilmingtonstar.com/apps/pbcs.dll/article?AID=/20060613/NEWS/606130323/1050&template=currents, accessed on 6th Feb 2007).

At a Round Table United Nations meeting, with Ministers including Australian Immigration Minister, Philip Ruddock, Pascal Smet, the Head of Belgium's independent asylum review board put forward a plan in late 2002 that every person in the world would be fingerprinted and registered under a universal identification scheme to fight illegal immigration and people smuggling (Sickler 2002).

The European Union favours "a single number identifier" (Bunney 2003, p. 10). Already Luxembourg, Finland and Sweden "give their citizens a single number that is uniquely applicable to all governmental applications".

2.6.5 Implantable microchips

Another identification alternative is an implantable chip. The chips are widely used as a pet identity device, which in America started voluntarily but is now mandatory if a pet is travelling overseas. The Ming newspaper in Hong Kong on 15 October 2004 reported that the European community recently proceeded with a cat and dog passport, which requires the implantation of the chip.

Implantation of chips is widely used in the agricultural sector as a means of identification, tracking and information collection. An example of the use is the monitoring of oestrogen levels in cows to identify the correct time to mate them. In an attempt to eliminate mad cow disease, the tracing of calves with chips has become compulsory (http://www.rfidgazette.org/2006/02/federal_governm.html, accessed on 10th March 2007). The styles of chips available will now be examined.

The human implantable microchip "contains a unique 16-digit electronic identifier. This unique number is used for such purposes as accessing personal medical information in a password-protected database or assessing whether somebody has authority to enter into a high-security area." (http://www.verichipcorp.com/content/company/corporatefaq#r7, accessed on 25th February 2007).

2.6.6 Radio Frequency Identification

Micro chips referred to as RFID (Radio Frequency Identification) can also be put in furniture or anything of value for tracking in case of theft. They can also be put in food to record temperature and location as it is shipped across the country (ElAmin 2006). A group led by the European Central Bank began work on embedding chips in the EURO bank note during 2005 (Yoshida 2001, p.1-3). A consortium of major manufacturers has sought to push the technology as a replacement for bar codes in everyday products ranging from cereal boxes to shaving cream cans, but the cost has not dropped low enough yet to make that feasible (ElAmin 2006).

Science writer and reporter Graham Phillips (2004) on ABC TV's Catalyst also asks "will a computer chip in the arm become compulsory for all of us?" "The entire population would essentially have super-ID cards implanted in them 24 hours a day" (Considine et al 2005, p. 385).

2.7 Microchips used as human identification

Clarke (1994) acknowledged the use of microchip for human identification purposes. "Subcutaneous Microchips for Human Identification (SMHId) has been created and used to isolate and differentiate this very specific human identification system from related areas and disciplines" (Covacio 2003, p. 2).

Michael et al (2005, p. 25) reports that “During the SARS outbreak, Singapore and Taiwan considered going as far as tagging their whole population with RFID devices to monitor the spread of the virus automatically”. With an implanted microchip under the skin, every human has a unique identification number and information about the owners is properly recorded (Clarke 1994).

Numerous identification chips are currently available and a representation of these will now be undertaken.

2.7.1 VeriChip

The VeriChip is a 12mm by 2.1mm radio frequency device about the size of the point of a typical ballpoint pen. The chip can be implanted via a simple procedure that could be performed in an outpatient or office setting. It requires only local anaesthesia, a tiny incision and perhaps a small adhesive bandage. Each VeriChip could contain a unique identification number and other critical data (Stewart 2006).

Chips embedded in passbooks and ATM cards will identify and profile customers as they enter bank lobbies. Chips embedded in U.S. passports can track citizens as they move about airport terminals and across international borders (Albrecht & McIntyre 2005).

As Young (2003, p. 70) suggested, in relation to the banking industry:

> "Any system requiring an implantable VeriChip would reduce the risk of theft of identify protecting related financial accounts and records. The threats of theft, duplication or counterfeiting of data are substantially diminished or eliminated with a system requiring the implantable chip."

Some companies like AmeriPride and Cintas are embedding this Radio Frequency Identification Device in company uniforms to track employees' behaviour (Albrecht & McIntyre 2005). Wal-Mart mandated its top one hundred suppliers to affix verichips to crates and pallets. Other retailers such as Albertsons, Target, and Best Buy (Albrecht & McIntyre 2005) followed the precedent. There are now sixty thousand companies operating under RFID mandates and scrambling to get with the verichip program as quickly as possible (Albrecht & McIntyre 2005).

2.7.2 Digital angel

Also available is the Digital Angel, which is a computer chip that measures just 11.1 millimetres x 2.1 millimetres including the microchip and its antenna, which is smaller than a grain of rice (Stein Washington Post, 2006). The assembly can be injected through a syringe and implanted in various locations within the body under the skin. The chip sends a signal to cell phone towers and satellites, it can tell the body temperature, pulse, heartbeat, and insulin levels. The chip also tells the location of a person anywhere in the world. All this information on a person would be available over the Internet. The chips are similar to those that are already implanted in about six million dogs and cats in

America (Stein, Washington Post 2006) to enable pet owners to identify and reclaim animals that have been temporarily lost or can be notified if their pet has been injured and has been taken to a veterinary facility for treatment.

Applied Digital Solutions maintain a website with archived chip-related news articles. Smith (2004) reported in Business Week that RFID tags in dogs and cats allow for 6,000 lost family cats and dogs each month to be reunited with their legal owners. The article concludes that with such technology already being used in the welfare and management of pets and livestock it is only a matter of time before humans will become part of the chipping process.

.

Currently Digital Solutions and other companies such as Verichip Corporation, use a tracking bracelet or wristwatch containing the chip (Sullivan, 2005). The chip transmits a signal to the Global Positioning Satellite. A person can be located within 60 seconds. According to Feder and Zeller (2004), Digital Solutions is shortly expecting to unveil the tracking microchip, which can be embedded beneath a person's skin.

2.8 Human implantation

The chip for humans differs from those used in animals mainly in the biocompatible coating that is used to stop the body rejecting the implanted chip. New Jersey surgeon, Richard Seelig, injected two of the Applied Digital Solutions chips into himself ('The Privacy Act: Your Privacy, your choice' 2002). He placed one chip in his left forearm and the other near the artificial hip in his right leg. He was motivated after he saw fire fighters at the World Trade Centre in September 2001 writing their Social Security numbers on their forearms with Magic Markers and he thought that there had to be a more sophisticated way of identifying people. Seelig, who serves as a medical consultant to the company, had the chips implanted in him for three months without any signs of rejection or infection.

Implantation has been described as "virtually painless" (Halamka 2005, p.331), due to the use of local anesthesia. In the process that Halamka (2005) describes, the chip sits in the posterior aspect of the user's right arm, between the elbow and the shoulder. Halamaka (2005) follows the process of the implantation of the chip and finds in the days after implantation "no pain, no infection, and no restriction of activities" (p.331). Halamaka (2005) describes that:

> "when a scanner is passed within 6 in. (15 cm) of container's arm, his/her medical identifier is displayed on the screen of a radiofrequency-identification (RFID) reader, and any authorized health care worker can turn to a secure Web site hosted by the manufacturer and retrieve information about his/her identity and the name of his/her primary care physician, who can then provide details of his/her medical history" (p.331).

Implantable chips are attracting global attention, as evidenced by the fact that even the Chinese Ming newspaper reported in Mandarin on 15 October 2004 that "Americans allow the implanting of a medical chip in the body for the first time" (p. 30). The article continued to state that the

> "FDA on Wednesday for the first time allowed a chip that can be implanted into a human body for medical purposes. Every chip has a unique PIN. The medical staff in the hospital only need to use the computer to scan the chip. They can then find out the history of the patients' medical record and personal information" (p. 30).

The article recorded the price of the medical chip as 1,200 Yuan, approximately $203 Australian at the time. The uses reported, included identifying the blood type or any allergies of patients implanted with the chip, and, for locating people with mental illnesses such as dementia, who are implanted with the chip.

Since two young girls, Holly Wells and Jessica Chapman were kidnapped in 2002, approximately 75% (Lane 2003) of English parents have considered implanted chips or a tracking device for their children to facilitate finding them if they were kidnapped. Professor Kevin Warwick of Reading University who implanted himself with a chip and is a keen advocate of this technology had publicly offered to chip an 11-year girl to demonstrate its effectiveness but was publicly criticised for making such an offer, by child welfare agencies and support advocates that he subsequently withdrew the offer. This indicates that while child safety is a major concern to parents there is still a strong resistance by the community at large for the acceptance of people being chipped in this

manner proposed by Professor Warwick (Lane 2003, p.1-3). Lane continues to explain that the community takes the view that the implantation would create a false sense of security and make children become complacent if they perceive the technology, which can fail, will take care of their personal safety. The long-term health effects of such devices, especially microchips transmitting signals from inside young bodies are also a concern for the community according to Lane. Lane argues that existing mobile phone technology is considered to play a similar role as the technology would help trace children's location by triangulating the signal if the phone has not been switched off (p.1-3). With respect to the implantable chip allowing access to medical records, Barclay (2004) documented the opinion that irrespective of the governments mandates patients would make their own minds up about the chips.

2.9 Real-time up-date

The chip would use a real-time up-dating facility allowing immediate documentation of expenditure or receipts to a master file enabled via satellite communications and establishing an up-to-date record. Transactions would be simultaneously added to a transaction file in case there is a need for subsequent verification, facilitating an audit trail. For example, an implanted chip would be scanned to make a payment for a purchase transaction and the information could be updated immediately in the bank. Currently, real-time up-date of information is achieved for implantable chip through Global Positioning Satellite (GPS), which relay the information via on-board cell phone technology to a data center, which then displays it on the Internet within seconds (Murray 2002).

2.10 Benefits of a verification mark

The ability to inject the chips opens up a variety of applications of human identification such as the high-security tracking of prisoners or parolees or the tracking of young children to protect against kidnapping. The September 11th, identification of body's issues could be solved by the chip, rather than the last-ditch efforts of victims using magic markers (Murray 2002). If a chip was implanted into all humans, this would make terrorists more easily detected and perhaps lead to their activities being prevented. These implantable chips would assist police to be more able to identify criminals.

An implantable chip would help in the fight against identity fraud as it would be required when establishing one's identity. Identity fraud is currently "one of the fastest growing crimes in the world" (Gee 2003, p. 68). Currently identity theft can be perpetrated when "some elements of a person's identity are obtained and used by another person for unlawful purposes generally for financial gain" (Gee 2003, p. 68). The type of information could include bank account details, credit card details, or motor registration details. The way of obtaining this information could be as simple as being stolen from a person's letter box or as sophisticated as hacking emails which invited customers of various banks to follow a link and log on to what appeared to be a legitimate bank site but was only being used to obtain details about the log on details of the customer. In November 2002 U.S. authorities "cracked the largest identity case to date with total losses estimated at US $2.7 million" (Gee 2003, p. 68).

Medical records could be included in the verification chip, preventing catastrophes such as administering drugs on an unconscious patient to which they may be allergic. The blood group of the patient could also be shown, making it easier in an emergency situation. The implanted chip could help adults with Alzheimer's disease or other mental and physical disabilities to be identified.

There would be a convenience factor; information such as driver's licence and contact details could be stored. As an example, Visa International's Executive Vice President for Australia and New Zealand, Bruce Mansfield stated that:

> "Fifty per cent said they would like to have Visa smart cards that can double as a driver's licence and significant numbers said they would like to use them to track expenses, to hold cinema tickets and as a frequent flyer card" (http://www.andreae.com/New_releases_of_interest/Selected_press_releases_2006_May.htm, accessed on 1st December 2006).

The implantation of a chip would make it possible in the future for all trading to occur electronically and there would no longer be a need to carry cash or credit cards to the surf beach or swimming pools, eliminating the chance of it being lost or stolen as you swim.

A chip would replace the need for a password which can be discovered. An example of another type of theft includes the scam at the Automated Teller Machine where recently thieves watched their victims re-enter their pass number, frustrated by the clear sleeve the thief had previously installed. The thief then works the victim's card out of the

machine using the plastic sleeve once the victim has left (Australian Competition and Consumer Commission - Scam Watch 2006). Visa International's Executive Vice President for Australia and New Zealand, Bruce Mansfield also said that "Australians had a positive attitude towards the introduction of smart cards because of their enhanced security features" (http://www.andreae.com/New_releases_of_interest/Selected_press_releases_2006_May.htm, accessed on 1st December 2006). The ability to trace using a verification mark could mean that credit card fraud could be eliminated completely.

Accounting for personal transactions such as budgets and taxation returns would become easier if the chip was used as part of a cashless monetary system. Taxation returns may well be done by government bodies themselves. Feige (2000, p.2) describes a system emanating from America where "tax is automatically assessed and collected when transactions are settled through the electronic technology of the banking/payments system", refereed to as the Automated Payment Transaction (APT) tax. Feige (2000, p.2) states that "the automated recording of all APT tax payments by firms and individuals creates a degree of transparency and perceived fairness that induces greater tax compliance". Feige (2000) describes a system whereby

> "the chip or software modification would create a virtual tax payment account (TPA) that is directly linked to every customer's financial account. The linked TPA would be required to maintain a positive balance somewhat in excess of expected tax payments. Every debit or credit to the primary account would trigger a corresponding debit in the TPA account equal to the debit amount multiplied by the flat tax rate. This amount of assessed tax would be electronically transferred to the account of the government. All taxes are automatically assessed and collected at the time the transaction is consummated by payment" (p.2).

The justification of the APT tax revenue collection system is to "eliminate the free use of government currency to defeat its revenue collection function by imposing a tax on all forms of final payment, including cash payments".

In a similar way that Feige (2000) describes, the verification mark could track payments to final consumers which would allow a sophisticated audit trail reducing the possibility for fraud. Non-financial information could additionally be stored which would make personal management of more than just finances possible.

2.11 Problems with implanted chips

Michael et al (2005, p. 22) report "academic papers on human transponder implants have surfaced, addressing specific themes such as legal and privacy concerns, ethical and cultural impacts, technological problems and health concerns".

> "Most alarming is the rate of change in technological capabilities without a commensurate and involved response from an informed community on what these changes actually "mean" in real and applied terms, not only for the present but also for the future. It would appear that the accepted standard nowadays is to introduce a technology, stand back to observe its general effects on society, and then act to rectify problems as they might arise" (Michael et al 2005, p. 33).

Civil libertarians, religious advocates and conspiracy theorists are concerned about the use of the information gathered and the functionality of the technology, claiming that the

auto ID technology will eventually lead to totalitarian control of the population (Michael et al 2005).

The potential for social control was discussed earlier in the context of cashless mediums of exchange. If this system were coupled with a more sophisticated system of collection using an implantable chip and all information about a person were consolidated, the issues of social control would be magnified.

The use of a verification mark will potentially greatly affect personal privacy. To some extent the information without a verification mark is fragmented.

System corruption could also effect the smooth operations of a system of cashless mediums of exchange. Heng (2004, p.1) stated that:

> "security is a key criterion for electronic payment systems. Critical issues are authorisation, authentication, privacy, integrity, theft and data corruption. The possibility of unauthorised access by third parties, misuse and manipulation must be excluded."

Heng (2004) continued on p.4 to state that "electronic payment systems must be prepared for the possibility of accidental data corruption."

2.11.1 Propensity to magnify an authority's control

The asymmetry of power between government and individuals is likely to increase with the introduction of a verification mark, which has the potential to increase the information collected and to consolidate existing information. The concern is the control

government has over society in a way that Bentham, cited by Foucault, describes well in the example of the panopticon or a viewing area which was set up and established to control the outspread of disease (Dreyfus and Rabinow 1982). This concept has been discussed earlier with respect to cashless mediums of exchange, however, the verification chip would further facilitate this to an unprecedented, even exponential, level. Elements of a system embracing the verification mark increase the similarity of the social implications, for instance, referring to the panopticon, Dreyfus and Rabinow (1982, p.134) note that "surveillance is based on a system of permanent registration" where the individual is "constantly located", all "complaints" and "irregularities" are "noted down and transmitted to the intendants". The verification chip could be thought of in this sense congruent with Foucault's extrapolation of the physical panopticon into social control.

2.11.2 Privacy issues

Additional information could be collected and consolidated as a result of the verification chip. People have different tolerances to privacy invasions. Up to 68% of respondents to a Community Privacy Survey conducted by the Federal Privacy Commissioner, felt comfortable with an increase in an authority's knowledge about them "if fraud and crime are being reduced" (Federal Privacy Commissioner 2004, p.6). For instance, if cashless mediums of exchange are encouraged or even enforced with the sophistication of technology the collection of such information is not only possible but also necessary to maintain the system with advantages such as reducing taxation fraud. The new taxation system introduced in 2000 under the guidelines of the Ralph Report (June 6 2000) is working towards a fuller reporting system and computer records seem to be the

logical extension. The rhetoric that there is only concern for those committing fraud reveal a failure to understand that every person is caught in the privacy dilemma. Some proffer the view that it is only the people with something to hide that would be worried about extra information being collected about them. Some have heightened levels of sensitivity. Jackson (2003) reported that 90 percent of people surveyed by the Federal Commissioner in 2001 "wanted businesses to seek their approval before using their personal information for marketing" (p. 22). The report was entitled 'Privacy and the Community, July 2001' (http://www.privacy.gov.au/publications/rcommunity.html, accessed on 21st December 2006). Interviews were conducted in May 2001 on 1,524 Australians aged 18 years and over which was the most comprehensive privacy research into the attitudes of individuals in Australia. The research found that even though participants exhibited a low level of knowledge and understanding in relation to privacy they showed a "high, and increasing level of interest in their own privacy" (http://www.privacy.gov.au/publications/rcommunity.html, accessed on 21st December 2006).

France-Presse (2006, p. 9) documented the development of the Life log Pod by Japan's telecom operator KDDI Corp that electronically record almost every event in a person's life. "The Life log Pod jots down every activity made through a cell phone or computer, including taking photographs, searching for a restaurant, listening to music and managing money" (France-Presse 2006, p. 9).

In establishing a monetary system based on an implanted chip it should not be assumed that a legal system will easily cater for naturally ensuing privacy issues. Brennan J in Halliday v Nevill (1984) examined the difficulty of the legal protection of privacy. He

acknowledges “tension between the common law privileges that secure the privacy of individuals” “and the efficient exercise of statutory powers in aid of law enforcement”. He contributed that “it is not for the courts to alter the balance between individual privacy and the power of public officials” (Morfuni 2004, p. 91)

2.11.3 Abuse

Given the ability of computer hackers to “have accessed top secret files inside the Department of Defence” (Mcllveen 2003, p. 5) it is reasonable to be concerned that a monetary system based on computer storage may be hacked into and tampered with. Whether the access resulted in temporary or permanent changes would be a concern. Third parties would gain unauthorised access of personal information via implanted chips with a reader and this will exacerbates the potential for improper use of information such as medical data (Barclay 2004).

The implanting of the chip does not preclude the physical interference with the chip. Perhaps a person could be kidnapped and the chip in their wrist or forehead could be misused. Barclay (2004) addressed other possible abuses concerning chips being removed, stolen, and put into someone else as a form of identity theft. A computer security and privacy expert highlighted RFID device that only sends out an ID number would not appropriately protect financial transactions and medical information (Barclay 2004). “The potential exists for building a device which will clone the ID number embedded in such an RFID device” (Barclay 2004).

2.11.4 Technology issues

A cashless society based on technology and an implantable chip would exaggerate the reliance on technology. If a predominantly cashless medium of exchange exists corruption to files could have a catastrophic effect. Data corruption is defined as computer data that when transmitted it arrives at the destination in a different format to the original source. The difference often results in the data being unusable to the recipient (Bagozz et al 1992).

Computer viruses, on the other hand, could be a potential problem that can occur with computer systems. A virus is a computer program "that attaches itself to a legitimate program data file and uses it to transport mechanisms to reproduce itself without the knowledge of the user" (PriceWaterHouseCoopers, Risk Management Forecast 2001, p. 236). Generally there are three types of viruses file infectors; system or boot-record infectors and macro viruses that infect data rather than programs.

Attacks on computer systems present a major problem with cashless money as they are so reliant on them. The Australian Newspaper, 4 June 1996, reported that cyber terrorists have amassed millions of dollars worldwide by threatening to wipe out computer systems. The article continued by stating that the City of London financial institutions are one such example as they have paid 400 million pounds to international gangs of sophisticated criminals (Macko 1996, p.156). Two underground publications have published code that allow hackers to launch "denial of service" attacks that can cripple servers serving any transmission control protocol-based function, such as web-hosting and e-mail. The United States General Accounting Office (1996, p. 4-9) outlines

the number of underground hacking groups that exist and how information is posted and shared on the Internet in planning and orchestrating "denial of service" attacks between/by individuals and/or groups.

Even a U.S. Air Force web site was hacked by a 13 year old who managed to manipulate credit card accounts (Aiken 1998, p.23). Tracing perpetrators can also be a difficult task despite the existence of a firewall. A firewall is a set of related programs, located at a network gateway server that protects the resources of a private network from users from other networks in addition to other security policies that are used with the programs (http://searchsecurity.techtarget.com/sDefinition/0,290660, sid14_gci212125,00.html, accessed on 21st December 2006). When an attacker breaches the firewall, it can be nearly impossible for the network administrator to determine what occurred, and which systems were compromised. Once entry has been gained evidence of an attacker's traces vanish if the intruder installs a password sniffer. "An intruder can compromise a system in many ways that can be difficult or impossible to detect" according to the Internet security newsletter in 2002 (http://infodev-security.net/handbook/part5.pdf, accessed on 21st December 2006). It is important that computer systems relied upon to protect personal and financial information are protected from abuse.

Control systems could, of course, be in place and effective back-up systems could be designed but the mere extensiveness of the potential for this problem makes this an issue worthy of thoughtful analysis. A focus on cashless mediums of exchange may have ramifications not thought of at this point in time. Consider the effect that computer generated purchase and sale of equities had on the 1987 share crash, Rubinstein (1988, p. 41) argued that computer trading, known as program trading, that was being used by

large institutional investing companies to order large stock trades when certain market trends prevailed, may have contributed to the crash (Itskevich 2002, p.1). Computers were programmed to sell equities if a certain low point was reached thus fuelling a downward spiral. The consequences of the computer had not been anticipated. If people's abilities to buy and sell are affected by a corruption of files real anarchy may result.

Advancements in technology create new challenges and there is an uncertainty about the level of protection afforded to information that is collected. Encryption softwares and other technological controls could at some level be used to protect users from hackers or abuse. Jackson (2003) states that "public key encryption makes it possible to 'sign' a document so that no one other than the recipient can open it". She also states that public key encryption can be used on the Internet to ensure confidentiality of information" (p. 29). The level of confidence argued by Jackson (2003) is surprising given the uncertainty of the advancement of technology and the determinations some have to break the encryption codes. This journey of the advancement of encryption controls and the attempts to break the controls would be expected to continue. Neiger (2002) investigated the available technology to protect businesses from "attack" (p. 54). Neiger suggests that protection is a moving target and needs to be secured on an "ongoing basis" (p. 54). It would be expected that much effort and finance would be expended to protect the information system supporting the cashless monetary system. It would be reasonable to expect the devotion of effort both financial and intellectual to break the implantable chip monetary system.

PriceWaterHouseCoopers Risk Management Forecast (2001, p. 149) states:

> “in practice, cryptosystems do not provide perfect secrecy. Rather, in a cryptosystem, the amount of work required to break the cipher is more than an attacker can manage or economically justify”.

As crypt-analytical research progresses hackers are more able to break codes “considered unbreakable”. The implantable chip would enable systems which provide sophisticated protection on the information collected. “Encryption technologies are a collection of techniques and applications for transforming information into a form that is impossible to read without special knowledge” (p. 150). Encryption and decryption require the use of some secret information which is called the key”. Such a key could be a digital signature which is “a digital code attached to an electronically transmitted message uniquely to identify the sender and guarantee message integrity” (p. 154).

Michael et al (2005, p. 26) indicated:

> "Another important aspect is the potential effect of the battery when using active responders …. When using electronic monitoring with current available technology, a battery is necessary to guarantee correct functioning of sensors when the transponders are outside the antennae field. If the transponder should break fluid may escape, and the question of toxicological effects has to be answered”.

Certification systems such as eSign, now known as Verisign Australia that is a provider of Internet trust services, have been adopted by various government departments. For instance, the Australian Customs Service, SPEAR – Land Victoria and EC: Land Exchange use such a system to identify individuals and businesses and “to make the

Internet and telecommunications networks more intelligent, reliable and secure in the area of connectivity and transactions" (Versign.Com 2006 – On-line web solutions statement).

2.12 Public position

The research considers individuals' acceptance of the implantable chip technology in the survey instruments. Civil libertarians would consider such a mark to be an invasion of personal liberty where some others would perceive that only the guilty who have something to hide would object to a permanent numbering system embedded on their body if it was not visible to the naked eye. The views of the financially literate represented by professional accountants in terms of allowing such a technology to culminate so personally are examined. The pertinent considerations to be used in this research to study acceptance of the technology and risks involved in such acceptance are identified via the development of acceptance theory and the use of a survey instrument.

Chapter Three: Review of technology acceptance theory

3.1 Introduction

Technology has made a great impact on both the business and private lives of many and there are many authors evident in the literatures who consider the issues of its adoption. For example, Ives et al (1983) considered acceptance of technology from a business perspective, Long (1993) and Medcof (1989) studied the relationship between the extent of use of information technology and task characteristics. Pentland (1989) considered the effectiveness of the computer as did Quinn et al (1987) who argued that adoption should "substantially boost the quality of output and productivity" (p. 27). Studies such as Aramis or the love of technology (Latour 1996) look at adoption from a sociology of technology perspective. Drifting technologies and multipurpose networks: the case of the Swedish cash card (Holmstron et al, 2001) have used theories such as the dynamics of large socio-technical systems - technology drift and actor-network theory to address how and why information technologies often need to change, relative to their initial conceptions, during implementation.

The current research considers technology adoption from a personal perspective. Many authors have considered the acceptance of technology and its personal impact. Rafaeli (1986) considered the correlation "of employees' attitudes towards working with computers" (p. 89). Kraut et al (1989) and Lepore et al (1989) looked at the quality of

work-life of computer users. Robey (1979) looked at computer-user satisfaction in the work place.

Whilst it is clear that there have been many studies dedicated to this area of technology and individuals, still as DeLone and McLean (1992, p. 1) state "the dependent variable in these studies – Information System success - has been an elusive one to define". However, from the literature it can be concluded that the two major approaches to considering technology which compliment consideration of the adoption of the monetary system described in this research are diffusion theory and acceptance theory which will now be considered in detail in order to develop a theoretical framework for the research.

3.2 Diffusion theory

The diffusion of innovation literature provides a set of characteristics that may affect an individual's opinion on adoption. Zaltman et al (1973, p 33 - 40) has examined the attributes of innovation including costs, return to investment, efficiency, risk and uncertainty, communicability, complexity, science status, perceived relative advantage and point of origin. Rogers (1983) has been extremely influential in this area and through a synthesis of previous studies identified seven attributes of an innovation being: relative advantage, image, compatibility, complexity, trial ability, visibility and result demonstrability. Authors such as Moore and Benbasat (1996, p 132 – 146) have also expanded the relevant innovation characteristics set.

Authors who have looked at information technology from the innovation decision perspective include Brancheau and Wetherbe (1990) and Rogers (1976), who both looked at the adoption of spread sheets focusing on the influence of information sources and internal communications within the information technology department. Cale and Eriksen (1994) did a longitudinal study on the factors affecting the implementation outcome of a main frame software package. Cooper and Zmud (1990) looked at adoption of material requirement planning from an organisational level and Hoffer and Alexander (1992) examined database machinery adoption and implementation including the implications for the management of information technology. Nilakanta and Scamell (1990) also focused on the process of diffusion of innovation in the context of database system development, including the extent to which information sources and communication channels facilitate the diffusion of data base design, how the influences of sources and communication channels influence diffusion channels and the rate of diffusion throughout the process. Parthasarathy et al (1998) examined post-adoption behaviour in the context of online services. Tornatzky and Klein (1982) examined factors considered to be determinants of information technology adoption. Karahanna et al (1999) make the point that "innovation theory is silent concerning how this attitude is formed and how it leads to the eventual adoption or rejection decision" (p. 185). This is, in fact, why current research decided to focus on acceptance theory.

3.2.1 Acceptance theory

One well established stream of research in the acceptance area followed the work of Triandis (1980) who believed that much of the work in psychology was "experiencing centrifugal forces of fragmentation" (p. 195). Triandis presents a theoretical framework focused on the "relationship of attitudes, values and other acquired behavioral dispositions" (p. 195). He does this by providing "centripetal forces" (p. 195) which include history, culture, ecology, personality and social factors. Triandis's model (1991) does not "propose a causal link between the cognitive component of attitudes with the effective component" instead "affect and perceived consequences are viewed as independent (but related) factors that influence behavior indirectly through intentions" (Thompson et al 1991, p. 68).

Thompson et al (1991) used a conceptual model "which builds upon Triandis's theory of behavior" to examine the "influence of prior experience on the utilization of personal computers" (p. 167). Thompson et al (1991) with the support of senior executives in various organisations selected and surveyed a specific business unit with a total of 325 completed surveys representing a response rate of 80%. The results suggested that "experience influenced utilization directly and that indirect influences were present but less pronounced" (Thompson et al 1991, p. 67) and indicated further "that moderating influence of experience on the relations between five of the six antecedent constructs and utilization was generally quite strong" (p.67).

Barki and Hartwick (1994) looked at user participation and considered their participation which provided a useful starting point for deciphering the precise nature of

the relationship among user participation, involvement, and attitude during systems implementation.

Also recognising the potential of the computer in business applications, Davis et al (1989) explored user acceptance of computer technology in business. He argued that researchers required a better understanding of why people accept or reject computers. Davis reviewed social psychology as a potential theoretical foundation for research on the determinants of user behaviour. Davis settled on Fishbein and Ajzen's (1975) and Ajzen and Fishbein's (1980) Theory of Reasoned Action (TRA) model as it was "an especially well-researched intention model that has proven successful in predicting and explaining behavior across a wide variety of domains" Davis et al (1989, p. 983).

Davis' (1989) contribution became very important as a major stream in examining information technology. Adams et al (1992), for example, had the intention to:

> "replicate previous work by Fred Davis on the subject of perceived usefulness, ease of use, and usage of information technology. The two studies focus on evaluating the psychometric properties of the ease of use and usefulness scales, while examining the relationship between ease of use, usefulness, and system usage" (p. 1).

Given the support this approach has in the literature both in information technology acceptance and social psychology and the greater conceptual contribution it was decided to pursue this approach in the current research.

3.2.2 A Mix of Diffusion theory and Acceptance theory

In the context of information technology, authors such as Agarwal and Prasad (1997), Chin et al (1995), Karahanna et al (1999) and Moore and Benbasat (1996) have used a mixture of both diffusion theory and acceptance theory. Agarwal and Prasad (1997) consider diffusion theory as well as acceptance theory in the context of their study of the innovation of the World Wide Web. They examine eight user perceptions which include a mix of both traditional innovation and acceptance literature constructs. For example, they use the ease of use construct from the technology acceptance literature which they argue to be similar to the definition in Rogers (1983): "notion of complexity and encapsulates the degree to which a potential adopter views usage of the target system to be relatively free of effort" (p. 61). In doing so they do not use the diffusion theory construct. They also use the relative advantage construct from diffusion theory agreeing with the Moore and Benbasat (1991) claim that it is similar to the notion of usefulness in the technology acceptance model and by direct inference that it takes its place, removing the need for the technology acceptance label.

Chin and Gopal in their 1995 article entitled "Adoption intention in GSS: Relative importance of beliefs" (p.42) argue the case for combining adoption theory and acceptance theory. Al-Hajri (2005) uses a mixture of theories when he examined internet technology adoption in the banking industry in Oman. He examined what he claimed were:

"the perceptions that tend to affect Internet technology adoption in the banking industry, namely:

- Perceived relative advantage
- Perceived organisational performance (not previously investigated)
- Perceived ease of use
- Perceived organizational/customer relationship (not previously investigated)" (Al-Hajri 2005, p.ii)

Karahanna et al (1999) also combines "innovation theory and attitude theory" (p. 183) as can be seen by the three "theoretical contributions" (p. 184) where they credited their research as being the first to "examine the different influences of a comprehensive set of innovative attributes on both adoption and usage behaviors" (p. 184). "A theoretical rationale is provided for differences across adoption and usage based on theories of attitude formation (p. 184)" and "a distinction is made between adoption and user behaviors (p. 184)".

The research of Karahanna et al (1999) which mixes adoption and acceptance theory is instructive from a number of perspectives. First, when they used acceptance theory they included in their research a subjective norm from Fishbein and Ajzen's (1975) and Ajzen and Fishbein's (1980) work. The subjective norm was removed from Davis' Technology Acceptance Model which was also based on Fishbein and Ajzen's (1975) and Ajzen and Fishbein's (1980) Theory of Reasoned Action. Second, Karahanna et al (1999) is representative of the view in literature, for example, Triandis (1980) which distinguish between pre-adoption and post-adoption. They state "from a conceptual standpoint, few empirical studies have made a distinction between individual's pre-adoption and post-adoption beliefs and attitudes" (Karahanna 1999, p.183). This "mark"

research takes the opportunity to examine the pre-adoption decision in isolation from any adoption decision as the monetary system described in this research is not currently operational. Most researchers which have empirically examined information technology using acceptance theory with precepts from the Theory of Reasoned Action and Theory of Planned Behaviour, such as Christensen (1987), Davis (1993), Davis et al (1994), Mathieson (1991), and Pavri (1988) have examined the acceptance after the adoption has taken place. Davis (1989) developed and validated new scales for two specific variables, perceived usefulness and perceived ease of use, which are hypothesized to be fundamental determinants of user acceptance. Davis et al (1989) addressed the ability to predict people's computer acceptance from a measure of their intentions in terms of their attitude, subjective norms, perceived usefulness, perceived ease of use, and related variables. Taylor and Todd (1995) on the other hand compared the Technology Acceptance Model and two variants of the Theory of Planned Behaviour to explain information acceptance behaviour.

The current research prepares for post-adoption research completely separate from pre-adoption, acknowledging the point made by Tornatzky and Klein (1982) that the factors that led to adoption may be vastly different to those factors that affect the continued usage. This prepares to close a gap in literature which Karahanna et al (1999) states "remains an unanswered question in information systems research" (p. 195) in a way not previously undertaken. Post-adoption research is referred to in the further research section of the thesis.

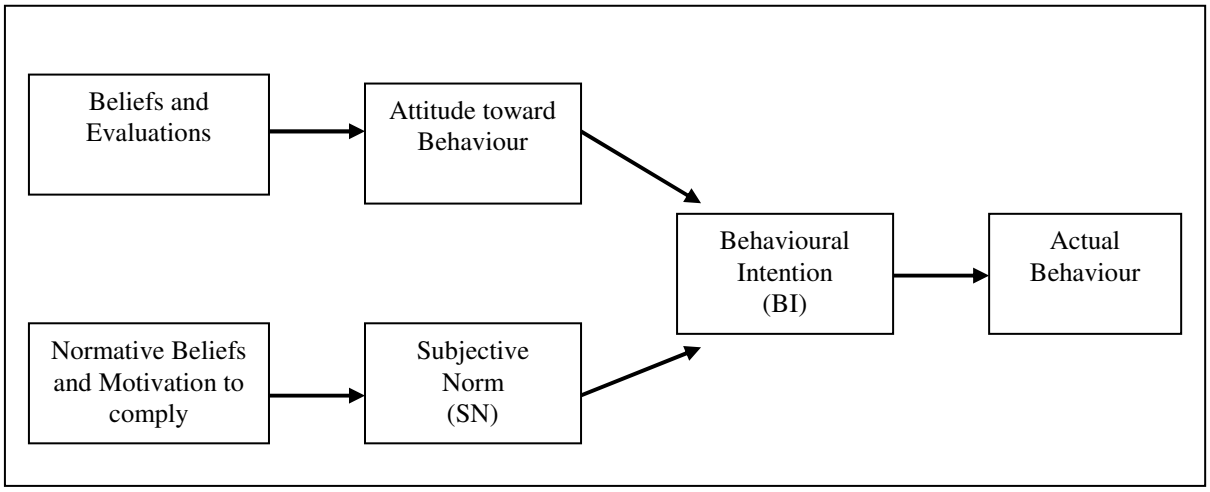
Unlike the approach taken by authors such as Agarwal and Prasad (1997), Karahanna et al (1999) and Moore and Benbasat (1996), it is believed a conceptually sounder

approach would be to focus on acceptance theory alone without mixing it with diffusion theory**.**

3.3 Theory of Reasoned Action

Fishbein and Ajzen's (1975) Theory of Reasoned Action shows beliefs and evaluations and normative beliefs and motivation to comply lead to attitude towards behaviour and subjective norm, respectively. The attitude towards behaviour and subjective norm both lead to the behavioural intention which is used to predict actual behaviour. Chart 3.1 Outlines the Theory of Reasoned Action.

Chart 3.1 Theory of Reasoned Action in diagrammatical form (Fishbein and Ajzen 1975, p.50)



Behavioural intention as represented in the penultimate box measures the strengths of a person's intention to perform a specified behaviour, which, in turn, gives an indication of the likelihood for the person actually to undertake the specified behaviour which is represented in the final box. Behavioural intention is affected according to the Theory of

Reasoned Action model by both the person's attitude towards behaviour and a person's subjective norm.

Attitude towards behaviour is defined as an individual's positive or negative feelings (evaluation effect) about performing the target behaviour. The attitude towards behaviour is a result of the person's salient beliefs about the consequences of performing the behaviour multiplied by the evaluation of those consequences. Beliefs are defined as the individual's subjective probability that performing the target behaviour will result in the consequence. Therefore, the attitude towards behaviour is a summation of the belief multiplied by the evaluation.

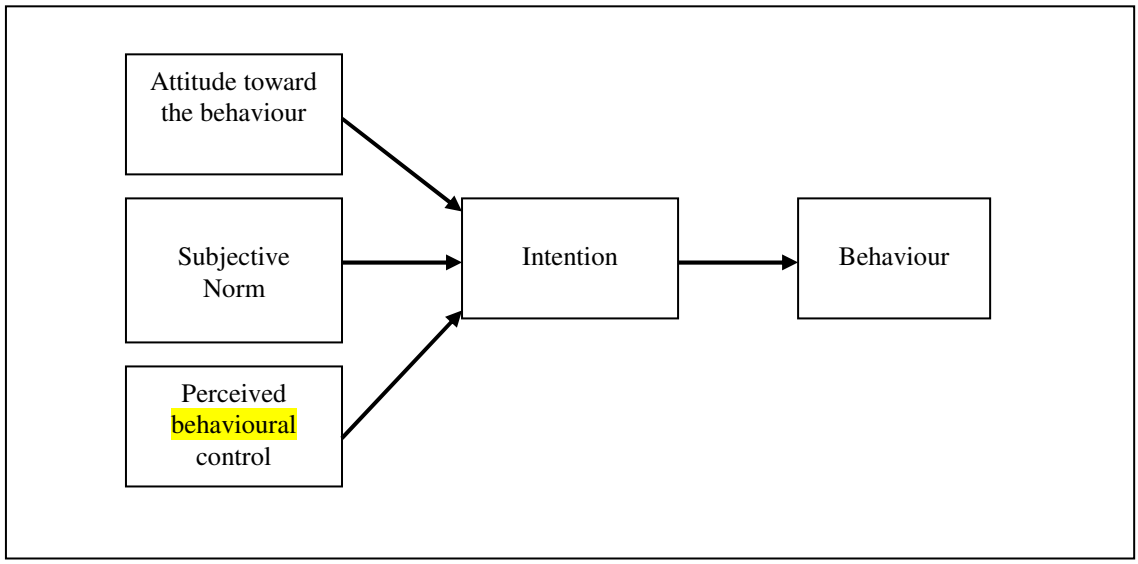
Subjective norm refers to "the person's perception that most people who are important to him think he should or should not perform the behaviour in question" (Fishbein and Ajzen 1975, p.302). A person's subjective norm is determined by the person's normative beliefs multiplied by the person's motivation to comply with the normative beliefs. These beliefs can be influenced strongly by people including friends or a peer group, family, co-worker, church congregation members, community leaders and even celebrities (http://www.fw.msu.edu/outreachextension/thetheoryofreasonedaction.htm, accessed on 15th December 2006).

3.4 Theory of Planned Behaviour

In an attempt to improve the Theory of Reasoned Action's ability to predict, Ajzen (1991) subsequently considered the difficulties of predicting behaviour of people who have incomplete volitional control. Volitional control occurs "if the person can decide at will to perform or not perform the behavior" (p. 182). A model was developed called the Theory of Planned Behaviour using the precepts of the Theory of Reasoned Action with the addition of the perceived behavioural control label to assist in the prediction of intentions and actions where there is incomplete volitional control.

Ajzen (1991) states "a central factor in the Theory of Planned Behavior is the individual's intention to perform a given behavior" (p. 181). Ajzen goes on to explain that "as a general rule, the stronger the intention to engage in behavior, the more likely should be its performance" (p. 181). Ajzen (1991) continues and explains that "a behavioural intention can find expression in behavior only if the behavior in question is under volitional control" (p. 182). Ajzen (1991) acknowledges that volitional control would depend on non-motivational factors such as "availability of requisite opportunities and resources (e.g, time, money, skills, and co-operation of others)" (p. 182).

Chart 3.2 Theory of Planned Behaviour (Ajzen 1991, p.182)



In explaining perceived behavioural control, Ajzen (1991) explains that a person may believe in general that their outcomes are determined by their own behaviour (internal locus of control), yet at the same time may have low perceived behavioural control. For example, a person may believe that their chances of becoming an airline pilot are very slim (low perceived behavioural control).

When talking of volitional control, Ajzen (1991 p.182) states that some behaviours "in fact, meet this requirement quite well". In the context of this research, consideration needs to be given to whether the behaviour examined falls within the requirement of being within the respondent's volitional control. It is thus to be assumed that the respondents and potential adopters are not required to pay for the right, are not denied the requisite opportunities to adopt and it appears the decision would be within their actual control over behaviour.

Taylor and Todd (1995) compared the Technology Acceptance Model and two variants of the Theory of Planned Behaviour to explain information acceptance behaviour. "Weighted least squares estimation revealed that all three models performed well in terms of fit and were roughly equivalent in terms of their ability to explain behavior" (Taylor and Todd 1995, p.2).

3.5 Technology Acceptance Model

The models developed by Fishbein and Ajzen (1975), Ajzen and Fishbein (1980) and Ajzen (1991) do not specify the beliefs that are operative for a particular behaviour, which requires the researcher to identify the salient beliefs regarding the behaviour under investigation which, in the current research, is information technology. In examining the literature surrounding the work of Fishbein and Ajzen (1975) and Ajzen and Fishbein (1980) in the context of information technology, the importance of Davis' (1989, 1993) Technology Acceptance Model was revealed. By way of illustration Taylor and Todd (1995, p. 145) state that "from this stream of research the Technology Acceptance Model has emerged as a powerful and parsimonious way to represent the antecedents of system use through beliefs".

For these reasons, Davis' (1989, 1993) Technology Acceptance Model has been chosen from the acceptance literature to be used as a basis for examining the acceptance decision of a monetary system using implantable chips. There is strong support in the literature for this approach including Ferguson (1997) who considered the effects of microcomputers on the work of professional accountants. Ferguson developed a model

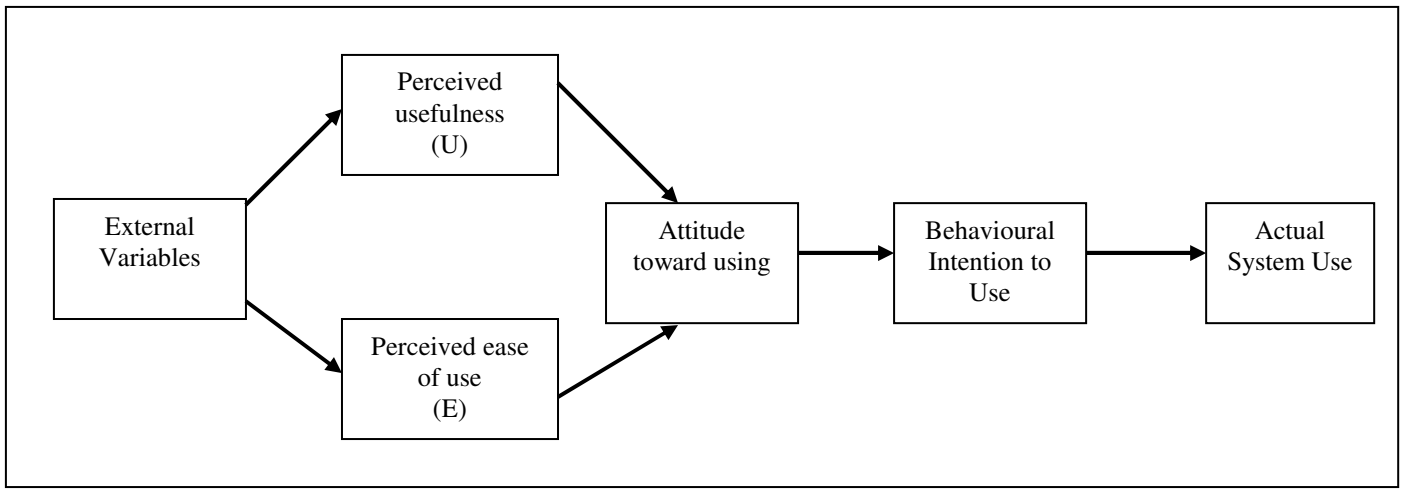
based on Davis' 1989 Technology Acceptance Model including "the interrelationships between perceptions, anxieties, attitudes, and microcomputer use and work outcomes of professional accountants" (Ferguson 1997, p. 41). The current study also examines accountants' views as they are informed about financial issues which are important in the adoption decision of a monetary system based on implantable chips. Ferguson (1995) applied Davis' Technology Acceptance Model directly in his study on the differential effects of human-computer interfaces on accountants using microcomputers where he looked at the perceived usefulness of microcomputers and perceived ease of use of microcomputers in relation to computer anxiety and the effect it has on the attitude to using microcomputers. Ferguson (1997) tested the premier accounting firms at the time with a sample of 157 representing accountants within the firms. He found that job satisfaction of professional accountants is directly affected by their "attitude towards using microcomputer" (Ferguson 1997, p. 41). Other support for the model includes those authors such as Adams, Nelson and Todd (1992), Mathieson (1991), Hendrickson, Massey, and Cronan (1993) who have replicated the Technology Acceptance Model.

Davis (1989) adapted the Theory of Reasoned Action model to tailor a model specifically for user acceptance of information systems, which he called the Technology Acceptance Model (TAM).

Davis posits that two particular beliefs are of primary importance for technology acceptance behaviour. These are the perceived usefulness of the computer technology for the intended tasks and the perceived ease of use of the technology. These two

beliefs, therefore, in accordance to the Technology Acceptance Model are the specified determinants of attitudes towards using the technology (as can be seen in Chart 3.3).

Chart 3.3 Technology Acceptance Model (Davis 1989)



.

The Theory of Reasoned Action asserts that any other factors that influence behaviour do so only indirectly by influencing attitude towards behaviour and the subjective norm. Davis (1989) uses this theoretical contribution from Ajzen and Fishbein (1975) to apply to technology acceptance decisions by including external variables, which contribute to the attitude towards behaviour, which, of course, is broken into perceived usefulness and perceived ease of use. Given the direct application of the general theory this would appear to be reasonable, although the Technology Acceptance Model does not include the subjective norm as recommended but rather it is removed from the model completely, the explanation given is set out below:

> "as Fishbein and Ajzen acknowledge, this is one of the least understood aspects of the Theory of Reasoned Action. It is difficult to disentangle direct effects of subjective norms on behavior intention from indirect effects via attitudes towards behavior" (Davis 1989, p. 983).

The newly developed model takes a different view to Davis (1989) and includes the subjective norm taking the view that Davis' (1989) argument is not sufficient to exclude the subjective norm.

3.6 Modified Technology Acceptance Model

The Modified Technology Acceptance Model returns to the precepts of the Theory of Reasoned Action (Fishbein and Ajzen 1975; Ajzen and Fishbein 1980) and uses the subjective norm component from that theory before making use of the Technology Acceptance Model (perceived ease of use and perceived usefulness) in an application of the theory designed to apply to the issue of society's acceptance of a verification mark. When the accounting community considers its acceptance of a verification mark as part of the technology of the described monetary exchange system, it is considered that Fishbein and Ajzen's (1975) subjective norm will be an important explanatory factor on behavioural intention. The internal implications of a permanent mark on their body may, for instance, bring about similar subjective norm issues surrounding the use of tattoos even if the mark will be invisible. The decision whether to have a tattoo may be expected to be impacted by the beliefs of a person's family members, friends or perhaps communities. The mark may be aligned to issues such as privacy, control and perhaps even religious issues. It could be agued that Davis' (1989) focus on technology acceptance in an organisational context has less call for an exploration of normative beliefs from the Theory of Reasoned Action model than this current study**.**

Davis's (1989) two salient beliefs deal with the benefits of the adoption of technology captured in the label of perceived usefulness and the cost in terms of the time expended to receive the perceived benefits, that being the perceived ease of use label. It is argued that the possible risks involved in adoption of technology should also be considered. In Davis's (1989) study, employees' acceptance was being tested and their interests in risks may well be restricted as the employer would carry the potential risks such as the financial risk of the adoption.

In dealing with technology acceptance, the literature has evidenced the importance of considering various risk factors in electronic transactions. For instance, Ho and Ng (1994, p.26) studied the risks and perceptions of electronic payment systems such as EFTPOS and the credit card, as compared to cash. Spence et al (1970) and Festervand et al (1986) both found non-store buying using technology is perceived to be "more risky" than retail store buying due, in part, to an inability to inspect products and the lack of personal contact. Another example is Van den Poel et al (1999) who investigated the effectiveness of the World Wide Web as a channel of distribution by, in part, considering the risk perspective and evaluating "risk relievers" (p. 254). Roselius (1971) examined purchase behaviour and the consequence of "the risk of suffering some type of loss" (p. 56). Chaudhuri (1998) studied "perceived risk" (p. 158) in relation to product classes.

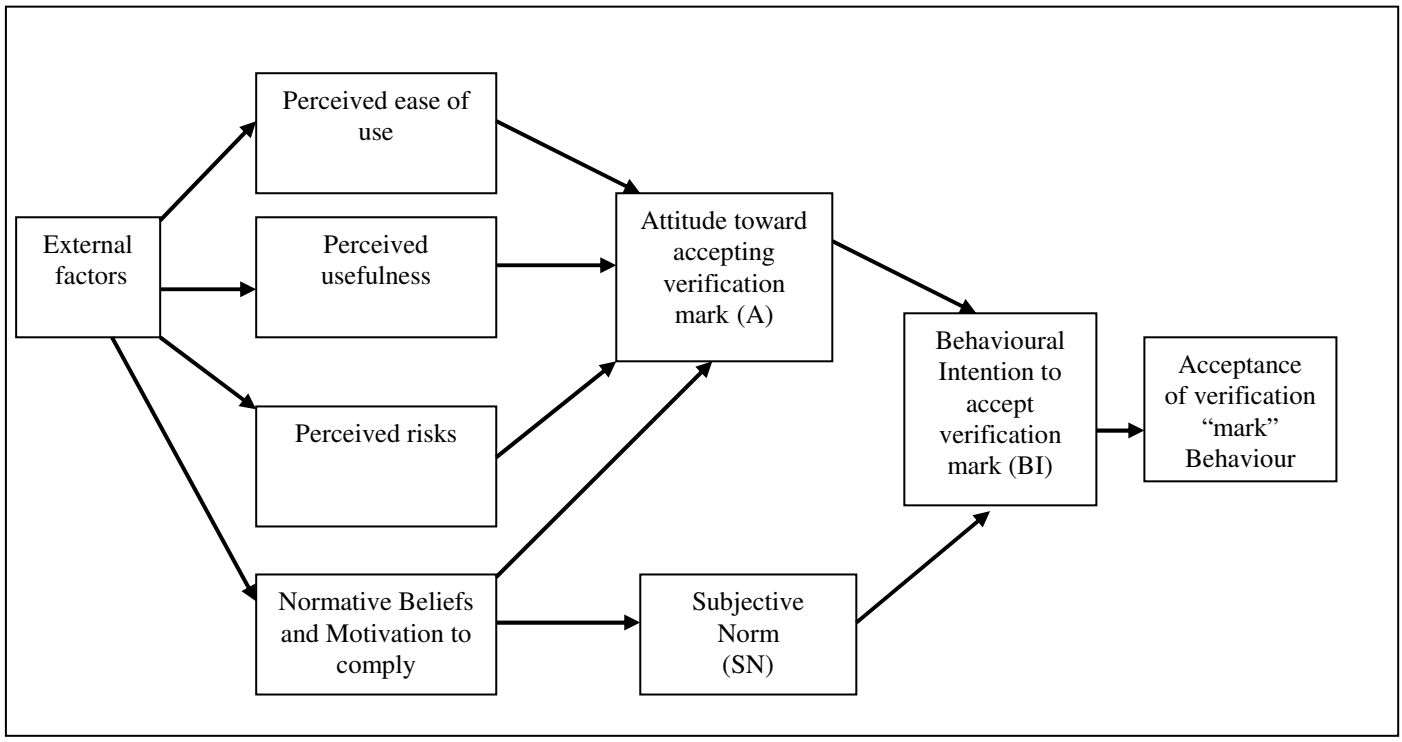
Further, Wang et al (2003) examined the determinants of user acceptance of Internet technology in the Taiwanese banking industry from an analysis of 123 phone interviews. They argued that the two TAM fundamental perceptions (perceived ease of use and usefulness) may not fully explain the user's behaviour; therefore, they included another

construct, perceived credibility. Wang et al (2003) noted this construct expresses security and privacy concerns. The authors suggested that it is important to focus on providing valuable function and trustworthy protection of security and privacy of the banking services on the Internet. Their findings also indicated that the formation of these perceptions could be managed through proper training and promotion rather than focusing on redesigning Internet banking technology.

The acknowledgment in the literature of risk influences in technology acceptance decisions has been accepted and has been found to be relevant in this research, especially given the potential importance and permanency of the "mark" decision. A perceived risk label was introduced into this current research on technology acceptance.

The Modified Technology Acceptance Model, as shown in Chart 3.4, is developed and used in this research as the theory base. The model includes four relevant variables that would affect a person's attitude and form their subjective norm: perceived ease of use, perceived usefulness, perceived risks, and normative beliefs and motivation to comply. The behavioural intention resulted from the attitude towards accepting a verification mark and the subjective norm would lead to the final behaviour of accepting a verification "mark".

Chart 3.4 Modified Technology Acceptance Model



Chapter Four: Description of the variables

This chapter provides descriptions for the four variables: Perceived Ease of Use, Perceived Usefulness, Perceived Risk, Normative beliefs and motivation to comply. Research question and hypotheses were then formed and discussed.

4.1 Perceived ease of use

The perception of ease of use was adopted as part of the contributions made by the Technology Acceptance Model (TAM) in its application of the Theory of Reasoned Action (TRA). Davis defined perceived ease of use as "the degree to which a person believes that using a particular system would be free from effort" (Davis 1989, p. 320)

Both TRA and TAM have strong behavioural elements that assume someone will be free to act without limitation when they form an intention to act. However, Bagozzi et al (1992) acknowledged that there are constraints such as limited ability which will limit the freedom to act, for instance, time constraints, environmental or organisational limits, or unconscious habits (http://en.wikipedia.org/wiki/Technology_acceptance_ model, accessed 2nd January 2007).

In its original application, that being a decision to accept a Windows environment over a DOS environment, the ease of use would have been important, as it was a major determinant in deciding how one might complete a job function in the most efficient way. The ease of use of the application is a major part of the cost in this style of

application as it equates with the expenditure of time on an on-going basis. In the verification mark application it is again considered important because it is felt that people want to feel that they can use the technology and will not be held up or embarrassed by the system. When trials of a cashless card were run in Sweden (Holmstrom et al, 2001) delays occurred when using the cards frustrating both vendors and shoppers alike. This problem was a major reason for the rejection of the system.

The proposed mark would require that you merely have to offer your mark for scanning once it had been implanted. The target of the research is Australian professionally affiliated accountants who are believed to be competent in financial matters and could easily conceptualise what is required of them. It is expected that accountants might perceive that a verification mark would be easy to use which would have a direct positive effect on the accountants' attitude towards accepting a verification mark.

4.2 Perceived usefulness

This was defined by Davis (1989, p. 320) as "the degree to which a person believes that using a particular system would enhance his or her job performance". Lin (2005) developed and tested a unified model that integrated constructs including attitudes, behaviour, and social influence. Her findings indicated that perceived usefulness was "a significant factor for predicting intentions" (p. 37).

> "In TAM, perceived ease of use has a positive impact on perceived usefulness, which has a direct impact on attitude toward usage. Further, intention to use is determined by attitude toward usage and by perceived usefulness" (Rotchanakitumnuai 2005, p.2).

Accountants may well believe that a verification mark would make accounting for transactions easier as it would create an electronic record of each transaction. The record may well be able to be accessed via a personal computer and used as the basis of financial management and taxation returns. A verification mark may have other advantages such as reducing the burden of having to carry a credit or identity card if it held information such as driver's licence details, medical information and contact details.

4.3 Perceived risks

Risks have not been contemplated fully in technology acceptance research using Davis' (1993) Technology Acceptance Model; possibly because risk may have been perceived as less problematic in dealing with issues contemplated by Davis such as a change from a DOS environment to a Windows environment in the context of a business. The personal nature of this current research makes risks of greater consequence to the decision maker and the permanent nature also increases the need for a risk analysis as the decision is not easily reversible and so the consequences and time frame are longer. The lack of risk consideration is addressed in the model adapted for this research. The risks can be considered from many perspectives.

4.3.1 Potential for social control

A category of concern may well be the lack of control individuals have once they have a verification mark, given its permanent nature. People may perceive that once they accept the technology they will have to accept changes to the system and the uses made of the information. Information can more easily be gathered and used for purposes outside the individual's control. This control may have a dehumanising effect on people. Do we want to live in a society so controlled? Whilst a less controlled system allows inequities due to cheats and skimming, at least liberty is maintained. Consideration should be made about a sophisticated system that would affect liberty and should not be used just because it is available.

With such a sophisticated identification system also come potential hazards. According to Foucault's argument in Rabinow (1982), the state tries to control society. The Sex Offenders Monitoring Act allows the electronic monitoring of sex offenders. On 16 August 2006 Dowsley reported that the notorious "Brian Keith Jones dubbed Mr Baldy, was arrested by prison officers after an electronic tag he wears warned them he was walking the streets of Ararat after 7pm" (p.1). There are examples where the government has considered using chips to control behaviour. For example, Haberfield (2004 p. 5) notes that some "poker machine players will have to register for a smart card under a bold new plan to curb problem gambling". The cards could impose time limits on the gamblers.

The more sophisticated the numbering system and collection of information, the more one can be controlled. The numbering system potentially allows physical controls. An

example might be an alarm system, which may be triggered by a chip when entering an illegal area. Financial controls may also be enforced such as the prohibition against spending money on illegal items or limits enforced on addicted gamblers. Apart from legal controls, moral control could also be exercised, for instance, tracing and entering into places like brothels. Perhaps, this could be seen as a positive outcome but it also could be perceived as controlling and a threat to personal liberty.

Kolberg (Crain 1985, p. 121) describes in his stages of moral development theory that a person may need to act outside "conventional" morals to arrive at a "post conventional" ethic whereby one may have to break the law in order to achieve a moral end. Nelson Mandela spent many years in jail having broken the law of the land because of his stance on apartheid issues (Mandela 1955-59).

4.3.2 Privacy

Strongly linked with social control is the concept of privacy. The very recording, potential to know or knowing, is sufficient to affect privacy. Perspectives can be changed because of information known about a person even if the knowledge is independent of social control. Integral to a cashless exchange is a centrally linked record of the exchange whether the recordings are kept by the government or businesses like banks. Consider the record-keeping involved in a financial exchange that involves a financial institution like a bank or credit union. Records are kept for various reasons including to validate the fact that the exchange has taken place and for dispute resolution. However, the perception may also arise that the verification mark would

decrease the amount of privacy accountant's have in their private and business financial affairs.

Opportunity International Australia Limited, for instance, uses bank account and credit card details to process transactions (http://www.opportunity.org.au/home.asp?pageid=1279F63F6C612F99, accessed on 21st December 2006). SGE Credit Union communications gather information about their customers relating to other products or services that the Credit Union or their preferred suppliers provided (http://www.sgefs.com.au/privacy.html, accessed on 21st December 2006).

Opportunity International Australia Limited documents that:

> "contact information such as: name; address; phone numbers and email addresses are used to process receipts and to keep you abreast of any issues or developments we may think you have an interest in" (http://www.opportunity.org.au/home.asp?pageid=1279F63F6C612F99, accessed on 21st December 2006).

Surprisingly it indicates:

> "Sometimes we collect some more personal information about you such as what church you attend; your age; your professional profile, date of birth etc. This information is used so we can notify you of any developments within Opportunity that may be of specific interest to you. For instance if you were involved in international banking, and the President of the World Bank were to speak at a function we were hosting, then we would contact you as a person with a specific interest" (http://www.opportunity.org.au/home.asp?pageid=1279F63F6C612F99, accessed on 21st December 2006).

This collection of highly sensitive information including the "church you attend" (http://www.opportunity.org.au/home.asp?pageid=1279F63F6C612F99, accessed on 21st December 2006) is justified on the basis of marketing the credit unions affiliated events which seems a poor reason to store such information. This information easily relates to the previous paragraph on social control.

Integral to a cashless exchange is a centrally linked record of the exchange. Consider the record keeping involved in a credit card statement. Records are kept to validate the fact that the exchange has taken place; it is necessary in dispute resolution, for account keeping amongst other worthy reasons. The taxation system is working towards a fuller reporting system making use of computer records. A perception may arise that a monetary system using a verification mark would decrease the amount of privacy accountant's have in their private financial affairs.

4.3.3 Abuse

Information collected as part of a cashless monetary system which, over time, would accumulate to an informative picture of a person's spending history could be abused either by an authority, or, by a person gaining unauthorised access, for instance, hackers. The increased convenience and speed of cashless mediums of exchange present challenges to a control system. If such a system is implemented the accessibility of records and the purpose of accessing the records may be a constant concern for some. Concerns may include the fear that records may be sold as a form of revenue generation. Issues such as the recent sale of credit card records to retailers without the direct permission of the cardholders together with the helplessness of the individuals to change

the situation is small evidence of a far worse potential for abuse. In 2005, the Australian Broadcasting Corporation alleged that "employees of a Gurgaon-base call centre are illegally selling personal information of thousands of Australians for as little as 10 Australian dollars (Rs335) per person" (http://asiamedia.ucla.edu/article.asp?parentid=28294, accessed on 6th February 2007).

There also may be positive perceptions about the ability of the verification mark to reduce various risks. Examples could include the reduction of the risk of someone finding out personal credit card details and using the numbers to perpetrate a fraud, or, the elimination of the risk of physically losing a credit, debit or smart card.

4.3.4 System corruption

Implantable chip technology related to a monetary system will be highly dependent on technology and there may be a perception that the system would be vulnerable to corruption.

4.3.5 Other risks

A monetary system based on implantable chip technology may invoke many other fears. There may be a perception that a verification mark could affect a person's health or create safety issues given that it would be implanted.

4.4 Normative beliefs and motivation to comply

An important part of the Modified Technology Acceptance Model is the subjective norm; an essential element transported from the original Theory of Reasoned Action. Those important to the individual are deemed to be an important explanatory factor on the intention to behave in a certain way. Who may be important to an individual will vary from person to person. Family members may be an important influence. Perhaps a parent's view is influential or perhaps it is the view of a spouse or a child. Organised groups are also renowned as powerful influences in individual's intentions to behave in a certain way. Perhaps it is the influence of the sports club or culture; perhaps it is the beneficent societies such as Rotary. Religious groups are perhaps the most renowned influences. As an example specifically related to the issue, the New International Version Holy Bible (1979, p. 313) in Revelation Chapter 14 verses 9-11 states that:

> "If anyone worships the beast and his image and receives his mark on the forehead or on the hand, he, too, will drink of the wine of God's fury, which has been poured full strength into the cup of wrath".

Many Christians are convinced this relates to an organised numbering system, which is referred to in this thesis. The strength of this statement creates enormous pressure despite personal beliefs of usefulness, ease of use and risks not to partake of the system.

The permanent nature of a verification mark distinguishes this research from other focuses of technology acceptance research which consequently lends itself to a greater examination of normative beliefs. As the issue involves personal rather than just a

business focus and the implications extend beyond the work place then it is suggested a greater focus of influence will come from personal rather than business sources. Family members, religious and community groups may be the source of such influence. The acceptance by work colleagues of the extension of technology may have a less dramatic influence on an accountant's preparedness to accept the verification mark than the support of a spouse or parent.

4.5 Research questions

The research question studied is: What level of acceptance would professional accountants have in adopting a cashless monetary system using an implantable chip technology and supported by global positioning satellite and a large computer system?

This research investigates the preconceptions of professional accountants of the acceptance of a possible monetary system based on personal verification using an implantable chip, global positioning satellites and a large computer system. The relevant parts of the transactional trail would be available to individuals, businesses and regulators and is designed to embrace a greater internal control over the monetary system to eliminate fraud whilst allowing a completely real time exchange system. A modified Technology Acceptance Model specially developed is used for this purpose.

The Modified Technology Acceptance Model used for this research is based on Fishbein and Azjen's (1975) Theory of Reasoned Action (TRA) and Davis' (1989) Technological Acceptance Model (TAM). An examination of the external factors required by the TRA

model as they relate to the use of technology applied by the TAM's used in addition to Fishbein and Azjen's (1975) Theory of Reasoned Action's subjective norm and a risk component. The research asks the relevance of these variables of the Modified Technology Acceptance Model in terms of testing the acceptance of the introduction or implementation of an implantable microchip as part of a greater system to record all financial transactions. This leads to four discrete elements which contribute to acceptance decision and behaviour, including perceived ease of use, perceived usefulness, perceived risk and the subjective norm.

4.6 Hypotheses

4.6.1 Statement of introduction

The hypotheses follow the order of the elements in Chart 3.4. Hypothesis 1 deals with the perception of ease of use of the verification mark. Hypothesis 2 deals with the perceived usefulness of the verification mark. Hypothesis 3 deals with perceived risks of using the verification mark. Finally, Hypothesis 4 deals with a subjective norm influence on the decision to adopt a verification mark.

4.6.2 Hypotheses

The following are the null hypotheses:

H1 The perception that a verification mark would be easy to use would not have a direct positive effect on an accountant's attitude towards accepting a verification mark.

H2 Perceived usefulness of a verification mark does not have a direct positive effect on an accountant's attitude towards accepting a verification mark.

H3 Perceived risks of a verification mark do not have an inverse effect on an accountant's attitude towards accepting a verification mark.

H4 The perception of a subjective norm will not have a direct positive effect on an accountant's attitude towards accepting a verification mark.

The decision to implant a chip to facilitate a cashless monetary system is expected to solicit strong reactions because of its invasive nature and significance of the decision. It is predicted that there will be a high number of respondents that will disagree with adopting the mark with a strong representation of respondents strongly disagreeing with its adoption. A proportion would be expected to be uncertain with less expected to agree to adopt the technology and very few strongly adopting it.

The emotional issues of risk dealing with privacy and control embraced in the model lead to the expectation of strongly disagree and disagree. The uncertain and agreed labels are expected to be more difficult for the model to predict.

Chapter Five: Methodology and questionnaire design

5.1 Survey

The development of technology has accelerated in the recent years. Perhaps because of the speed of the developments there is a lack of research into the acceptance of the technology by the financially literate. The theoretical underpinnings of this research designed to develop the testable hypotheses lead to the collection of a representative sample. Roberts (1999) observed that the survey method "proposes the pattern among the variables of interest" (p. 55).

There is minimal research into the acceptance of the technology that could facilitate a cashless monetary system by the financially literate. This lack of research drove the research method towards a broad-based questionnaire style, reaching greater numbers than would be possible in interviews, focus groups or case studies given the restriction of time and money. Chongruksut (2002) acknowledged that the mailed questionnaire survey is the most appropriate to gather a large sample of a population at low cost which is relevant to the current study. This style of survey has been pursued even though De Vaus (2002, p. 123) warned that the response rates are "typically lower than telephone or personal interviews".

The knowledge sought in this research is more general in nature than might be sought by a smaller group of specialists in the area. With the expectation that many people in society will be lead by the views of the reputedly financially literate, the group this

research aims to survey are from those that represent the financially literate, rather than experts in the specific field of technology.

5.1.1 Source selection

Professional accountants from Australia were seen as appropriate to survey, as they would be perceived as qualified to answer questions which relate to financial issues involved in a verification system. Surveying informed individuals will undoubtedly add to the knowledge in this area. If the adoption of the technology is then considered to be an appropriate course of action then convincing people of the technology's worthiness becomes important for an authority and once again informed peoples views will hold weight. Further, should the technology adoption progress, pre-consideration of people's views should reduce adoption difficulties and make diffusion easier.

The research is designed to focus on accountants with professional qualifications. The criterion used for the financially literate in this research was that the accountants were to be full members of an Australian professional body or its equivalent, with a degree qualification or its equivalent. Certified Practising Accountants and Chartered Accountants were selected as the target population in this research. Accountants from the National Institute of Accountants did not necessarily fulfill the degree requirement and publicly available information did not allow the study to distinguish between those who had this qualification and those who did not. For this reason, the National Institute of Accountants was not included. According to the Federal Rules of Evidence 1971, the judicial standards for survey research indicate that "the population should include all

relevant respondents and exclude inappropriate, acknowledgeable, or unconcerned respondents" (Van der Stede et al 2005).

The target population was 135,000 (as identified in Table 5.2). Whilst Morgan (1990) documents that a sample of 200 to 300 respondents achieves face validity in this context, 523 of the target population were selected as the representative sample, as it was considered to be "substantively significant" (Sapsford 1999, p.93) and "intuitively justifiable" (Morgan 1990 p.63). The long process of selecting databases, appropriate sampling method and the sample is explained in the remaining section of 5.1.

5.1.1.1 Selection of database

In gaining an understanding of the relevant accountant populations, two options were available. Using Australian Bureau of Statistics information or accounting body information. It was decided to use the professional body's information as the Australian Bureau of Statistics information did not specifically address accountants and information could only be inferred. Definitional issues arose as well, given that an accountant is not a legal term and specific criteria had been applied to the research.

The Melbourne Big and Telstra directory databases were therefore not selected as they do not distinguish between professionally qualified accountants and unqualified accountants, given that accounting is a not a legal term. Application was made to CPA Australia and the Institute of Chartered Accountants Australia (ICAA) for permission to access their databases. Both rejected the application originally, citing the new privacy

legislation as being the obstacle that prevented them from doing so. This database included information on all accountants that were their members.

The ICAA did not entertain further discussion on the issue. CPA Australia were prepared to consider the application further if application was made to the CPA research grant scheme. Sometime later a decision was made that access to the database would not be permitted.

Publicly available databases were the remaining option. These databases included only accountants that were in public practice which limited the extent of the examination. Accountants available on CPA Australia's and the ICAA publicly available databases had the advantage of not only registering full members but it also listed members with public practising certificates. This latter group were more likely to be principals and au fait with the needs and views of the public than perhaps niche' groups in the total member database which are likely to include other members such as academics or public sector accountants.

Given the selection criterion of 'financially literate', the use of the CPA Australia's and the ICAA's publicly available databases was expected to result in a representative sample that fitted the research requirements. It was decided to proceed with this option. All accountants on the publicly available websites, "Find a CPA" and "Find a CA" met the definition of "financially literate" as defined in this research being undertaken.

With the "Find a CPA" database a full list of all accountants could be downloaded from which a sample could be drawn. This database did not allow the selection of a particular

type of accountant, but, did provide information on the industry in which the accountants had experience, for example property services, agriculture or manufacturing. With the "Find a CA" option, restrictions existed on the database that forced the selection of a state or territory, a postcode and a type of Chartered Accountant, for example, a tax accountant. In using the database, ten randomly selected accountants are furnished with each request and are selected from members who fit the criteria. A second request with the same criteria provides another ten random selections if more than 10 members fit the criteria offered.

As indicated, a postcode was needed to be entered to make a selection from the "Find a CA" database, the Australian Bureau of Statistics publication "Local government area populations for each state and territory" was used to aid selection, the most recent publication at the time being the 30th June 2002 edition.

The spread of local government areas was broad, New South Wales had 173 areas, Victoria had 78, Queensland had 57, South Australia had 68, Western Australia had 42, Tasmania had 29, Northern Territory had 10 and the Australian Capital Territory had 1. If a postcode was randomly selected from the various states and territories a local government area such as Hammond with an estimated residential population of only 208 would have the same chance of being selected as a local government area such as the Gold Coast with an estimated residential population of 438,473.

To avoid a concentration of smaller localities it was decided that accountants would only be drawn from local government areas where the population was at least 50,000. The number of local government areas fitting this criterion was as follows, New South

Wales 44; Victoria 36: Queensland 17; South Australia 9; Western Australia 12; Tasmania 1; Northern Territory 1 and the Australian Capital Territory 1.

5.1.2 Survey numbers selected using CPA Australia and ICA demographics

Member demographics were important in order to select proportionately from the two accounting bodies chosen. The ICAA's member numbers were taken from the 2002 Annual Report, although no break-down information on member categories and locations were available. In defining the population for CPA Australia members, the demographics from their annual report (2000, p. 2, 3, 9 and 13) were used and extrapolated into the then current year, being 2002. This was necessary, as the CPA Australia Annual Reports in the later years did not contain member numbers, and only limited demographic break-up information was available. There were also no details of State and Territory break-downs.

Table 5.1 Total number of members in the Institute of Chartered Accountants and CPA Australia

	CPA	% increase	ICAA
1997	84,116		
1998	86,881	3.287	
1999	90,208	3.829	
2000	91,882	1.855 An average of 2.99 increase or ≈3%	
2001	94,638*		35,670
2002	97,477*	5.194	37,523

* Estimated membership based on 3% increase.

The total number of accountants in 2002 in both professional bodies based on reconstructed figures was 135,000 (97477 for CPA Australia [72%] and 37523 for ICAA [28%]).

An objective of the survey was to establish a representative sample of Accountants within Australia and based on membership size in these locations. Details regarding this were necessary. As mentioned, membership by region was not supplied in the ICAA's Annual Reports so the CPA Australia, breakdown was used in an encompassing way.

Table 5.2 Membership by regions (from CPA Australia 2000 annual report)

	Total	%
ACT	2,130	2.3%
ASIA	16,757	18.2%
NSW	24,253	26.4%
NT	351	0.3%
QLD	9,795	11.0%
SA	4,117	4.4%
TAS	988	1.0%
VIC	24,217	26.3%
WA	6,833	7.5%
Other overseas	2,441	2.6%
Total	91,882	100%

As the research is confined to Australia, the overseas component of the members by region was removed from Table 5.2 and Table 5.3 identifies the numbers of members that are based in Australia. Initially, the sample was distributed directly in accordance with the percentage of members in each State or Territory. The strict adherence to the percentage proportions resulted in small sample sizes for Tasmania and the Northern Territory. A minimum of fifteen samples for any State or Territory was adopted to solve

the problem. This decision, together with rounding issues, resulted in a total sample size of 523 (see Table 5.3).

Table 5.3 Membership - Australia only (constructed from table 2)

	1	2	3	4
	Total	%	500	500 (at least 15)
ACT	2,130	2.90%	15	15
NSW	24,253	33.30%	167	167
NT	351	0.50%	3	15
QLD	9,795	13.50%	68	68
SA	4,117	5.70%	29	29
TAS	988	1.40%	7	15
VIC	24,217	33.30%	167	167
WA	6,833	9.40%	47	47
Total	72,684	100%	506	523

(Note: Column 2 is the percentage of members within the states and territories, and Column 3 represents the calculation rounded to the nearest whole number. Column 4 is the extension of column 3 but with a minimum of 15 per state or territory. Table 5.4 utilises this breakdown and distributes the distribution between CPA and ICAA.)

Table 5.4 Membership - Australia only

	State or territories	ICAA	CPA
	See table 3	28%	72%
ACT	15	4	11
NSW	167	47	120
NT	15	4	11
QLD	68	19	49
SA	29	8	21
TAS	15	4	11
VIC	167	47	120
WA	47	13	34
Total	523	146	377

5.1.3 CPA demographics

In order to gain an appreciation of the demographics of professional accountants in Australia the following information pertaining to CPA Australia derived from CPA Australia's Annual Report (2000) are documented. The ICAA Annual Report did not contain such details.

Table 5.5 Ratio of women to men in CPA Australia

Ratio of women to men		
	%	*%*
1990	29.2	70.8
1991	39.3	60.7
1992	36.7	63.3
1993	39.3	60.7
1994	41.6	58.4
1995	43.3	56.7
1996	44.8	55.2
1997	45.7	54.3
1998	46.6	53.4
1999	48.3	51.7
2000	49.6	50.4

Member status	*%*
Fellow	12
CPA	49
Associate	39
Total	100

Age demographics	*%*
<30	18
30-39	30
40-49	23
50-59	16
60+	12
Unknown	1
Total	100

Employment profile	**%**
Commerce and industry	49
Retired	8
Public practice	18
Public sector	15
Academia	3
Not for profit	2
Other	5
Total	100

Years of membership	**%**
<5	23
5-9	25
10-14	14
15-19	10
20-29	14
30-39	9
40-49	3
49+	2
Total	100

5.1.3.1 CPA Australia member selection

Having determined the number of CPAs to be selected, the actual sample was selected randomly. As the "Find a CPA" database is arranged alphabetically into states and territories then randomness was established via the systematic selection. A dice was rolled and the resultant number, two, became the random starting point for the systematic selection of the accountants on the database. The dice was rolled again and the resultant number, four, became the interval of selection. The selections were made from the "Find a CPA" database until the requisite amount of selections from the various state or territories was made. According to Diamond (2000, p.237), "probability sample increases the representativeness of survey results, thus allowing inferences to be

made from the sample to the survey population within a calculable margin of error", and thus minimises the sampling errors and improves the external validity.

5.1.3.2 Institute of Chartered Accountant's selection

A different selection system was used on the "Find a CA" website which revolved around postcode. The degree of sophistication for random selection needed to be increased. The random number generator function in Microsoft Office Excel was used to randomly select which postcode and the type of accountant (audit, financial planning specialist, general accounting, tax, insolvency) that would be used for the selection of members in each State and Territory as part of the database requirements. Once the key elements were entered into the database, the selections generated (a maximum of ten accountants each time) were used.

5.2 Questionnaire design

Whilst it is acknowledged that a structured questionnaire restricts the depth of data collection, it is considered justifiable as the research relates specifically to acceptance and the questionnaire is used to draw inferences about the population in accordance with the rules established by Roberts (1999) in his article 'In Defence of the Survey Method: An illustration from a study of user information satisfaction'.

Colombo's (2000) advice was taken to expend significant effort on the survey design in order to increase the response rate. De Vaus' (2002, p.123) advice was also relied upon

to minimize follow-up procedures. De Vaus advised that surveys need to be easy to follow with questions that are self-explanatory for the respondents in order to avoid bias. Response rate was increased by sending a second questionnaire as part of the follow up process and a comparison between early and late respondents was performed, and detailed later in this chapter.

It was decided to couple open-ended questions with the Likert-scale questions which are mainly designed to collect quantitative data to be used in the analysis. Creswell (1994), Fielding and Fielding (1987) and Gray and Densten (1998) agreed that the confidence in the conclusion of research based on questionnaire increases by collecting both quantitative and qualitative data. In the use of both open-ended questions and Likert-scale questions, the closed responses will be complemented with the richness gained from responses where the respondents chose how to word their answers.

5.2.1 Scale

Bowers (1976) acknowledged the validity of the Likert-scale used to analyse a number of "human resource issues including the central role of the work group, participative decision making, communication and the linking pin function, supervision and peer group loyalty" (Gowland 2000, p.26).

"The utilisation of the Likert-style of questioning is designed so that the researcher can measure the same variable and sum the responses to the questions" (Gowland 2000). "Research regarding optimum survey designs has suggested scale designs and the

number of items used affect the reliability and quantity of responses" (De Lange 2000, p.123).

In this questionnaire, three types of measurement scales are used: interval scale, nominal scale and mainly ordinal scale. Interval scale and nominal scale are used in collecting information about the respondents including age, salary, length of service and gender. The majority of the questions are ordinal to measure the respondents' attitudes towards the change of technology in accordance with Neuman (1997) and Zikmund (1991) who agreed the use of ordinal scale is appropriate when a measure requires ranking according to magnitude.

Likert-scales are widely used and most common in survey research (Neuman 1997). Mitchell and Jolley (1988) took the view that a Likert-scale is equivalent to interval data in that a subject giving a scale of 5 for strongly agree compared to a subject giving the scale of 4 for agree differ by approximately the same amount as a person who gives a scale of 1 for strongly disagree compared to a scale of 2 for disagree. The argument includes the fact that there is a psychological interval between each consecutive number.

Gowland (2000) states that the use of a scale of five allows respondents to believe they were not forced to select an answer that did not represent their true position. A five point scale was therefore believed to be sufficient for the purpose of this research. The scale still retains the nature of ordinal data which affects the statistical analysis. For example, ordinal data should be analysed using a Multinomial Logit regression rather than the OLS regression method. This approach was therefore used. A multinomial logit model generalizes logit models in which there can be more than two cases. It is a

statistical model or econometric model often used for data in which the response is often a set of choices as is the case here.

5.2.2 Questionnaire structure

The questions were motivated by literature. The literature contributions and the resultant questions are detailed in the following relevant sections of this chapter. The questionnaire was divided into distinct sections with a total of 49 questions. Descriptive information was gathered about the respondent in section A (Q1-7), these characteristics are used in the analysis for section B - E. Responses relating to the model were then obtained progressively. Ease of use questions were contained in section B (Q8-14) with all questions being closed except for Q14. Questions relating to "usefulness" were contained in section C (Q15-19) with Q19 being the only closed question. "Risks" were dealt with in section D (Q20-35); the final question in this section was the only open question. Questions pertaining to "normative beliefs" were contained in section E (Q36-42) with Q39 being the only open question. Questions relating to "acceptance" appeared in section F (Q43-49) which also contained questions relating to the respondent's belief about the status of existing technology that would allow the mechanics of a monetary system revolving around an implantable chip with Q49 being the open question.

5.2.2.1 Test of consistency

The decision was made to use a mailed questionnaire. Summers (1969) notes that respondents may be biased and errors can result from the tendency of people to answer a question falsely through deliberate misrepresentation or unconscious falsification,

referred to as respondent bias. The bias could be intentional or unintentional made by the respondent during the survey. The test of consistency helps identify any possible intentional falsification while pre-testing helps to prevent unintentional bias.

In this survey, the styles of question were mixed in the questionnaire for the purpose of testing consistency. For example, there were three styles of closed questions relating to risk as illustrated in Table 5.6. This makes it possible to test for consistency in order to further strengthen the internal validity of the survey.

Table 5.6 Questionnaire by style

Style	Survey Question	Reference
Style A: Related to the perception that the implantable chip would increase risks in the respondent's life, for instance, the level of control exerted on their life by the government.	20	5.2.6.1
	21	5.2.6.1
	22	5.2.6.1
	23	5.2.6.1
	24	5.2.6.1
	32	5.2.6.4
	33	5.2.6.4
	34	5.2.6.5
	35	5.2.6.5
Style B: Questions asked about the mitigation	28	5.2.6.3

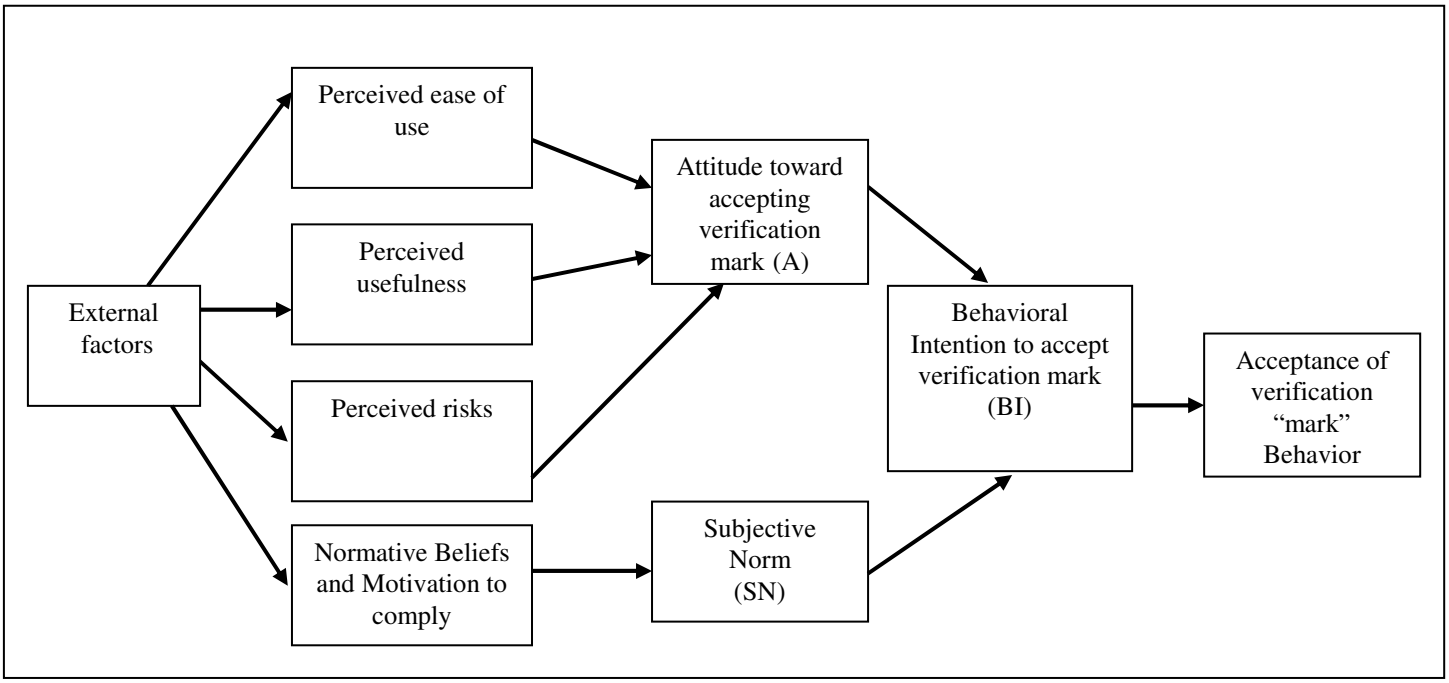
of risks currently perceived due to having an implantable chip, such as the reduction of fraud because the chip is always implanted in the person.	29	5.2.6.3
	30	5.2.6.3
Style C: Questions explored the comfort the respondent felt with measures designed to protect people from the perceived new risks that may arise due to the implanting of a chip. Such measures included constitutional, legislative or encryption software protection.	25	5.2.6.2
	26	5.2.6.2
	27	5.2.6.2
	31	5.2.6.3

The relationships among variables were established to facilitate the test of consistency of responses. The ease of use, usefulness and subjective norm variables were expected to have a direct relationship with the acceptance of the implantable chip technology whilst the risk variables were expected to have an inverse relationship. A perception that having an implantable chip would increase risks was expected to have an indirect relationship with the person's intention to accept the chip. Finally, the subjective norm component was expected to have a direct relationship with acceptance, that is, if those that were important to the respondent felt the technology would be easy to use or useful, then that would positively affect the respondent's likelihood to accept the technology. Similarly, if those important to the respondent felt the risks resulting from the technology were increased and could not be controlled, then this would have an indirect effect on the likelihood of the respondent to accept the technology. The test of consistency from one question to another provides evidence that support the fact that participants had answered the survey in a consistent manner.

5.2.3 Arrangement of questionnaire structure

Close scrutiny of the model shows that it states that perceived ease of use, perceived usefulness and perceived risks all influence the "attitude towards accepting" the verification mark (refer to Chart 5.1). The normative beliefs and motivation to comply lead to the subjective norm. The "attitude towards accepting" and the subjective norm then help to explain the behavioural intention to accept the verification mark.

Chart 5.1 Modified Technology Acceptance Model



5.2.4 Perceived ease of use

The Perception of Ease of Use came from Davis' (1989) Technology Acceptance Model.

In applying the concept of ease of use to the adoption of a "verification mark", administration, both from the perspective of gaining the mark and using the mark were examined, including the medical implementation procedures. Literature described the implanation process as requiring a "local anesthesia, a tiny incision and perhaps a small adhesive bandage" (http://www.lot49.com/2001/12/applied_digital_solutions_intr.html, accessed 17 Dec 2000). The process is not expected to be perceived as difficult for the accountants surveyed.

The US Department of Transportation in their study of "Driver acceptance of Commercial Vehicle Operation (CVO) technology in the motor carrier environment" (Golob et al 2001) gave an insight into the administrative procedures likely in the adoption of the implantable chip. The article highlighted the importance to consider the administrative process in studying technology acceptance. Literature indicated the administration process associated with the implantable chip would not be difficult for the accountants surveyed. With respect to accessing the mark, literature indicates that accountants would find the process relatively easy. Peet (1999) indicated that "human-computer interaction research continues to ease access to available data". The ease of updating is considered by Phillips, G. (2004) who discussed the use of scanner over patients implanted with microchips to gain immediate access of medical information, driving the question on this issue. Heng (2004) highlighted authorisation as being one of

the important issues in considering a system of cashless medium of exchange which led to a question regarding the ease of separating these transactions via levels of authorisation. An open question was included in the survey to identify other potential factors not considered in the closed survey. This open question facilitates the research by providing an opportunity to gather qualitative information

It was expected that the accountant might perceive that a verification mark would be easy to use which consequently would have a direct positive effect on the accountants' attitude towards accepting a verification mark. The survey described the implementation procedure in the context of ease of use examination. An extract of each question under Section B: Ease of use is provided below.

Question 8 deals with the ease of the implanting process, Question 9 deals with the ease of the administrative process whilst Question 10 deals with the ease of the accessing the "mark". All of these aspects of the process would be a necessary part of using the microchip which may be considered difficult by some people.

The concept of using a scanner linked to a global positioning satellite may be confusing to some people especially if it was linked to the purchase and sale of items, therefore, Question 11 deals with the ease of the updating the "mark". Using a phone or computer to pay bills may be an expectation for many people therefore Question 12 deals with the difficulty of using a scanner to access the implanted chip. People may get confused about private and business transactions therefore question 13 deals with the ease of separating these transactions via levels of authorisation. Question 14 being the open

question was set up to collect the potential factors people presumed that make a “mark” difficult to use.

Extract of questionnaire: Section B: Ease of use

Your perceptions are being sought for the following questions on a scale from:

SD = Strongly Disagree to SA = Strongly Agree

Please tick the box that best fits with your reaction to each of the following statements.

A verification mark or “mark” refers to a microchip that is implanted under a persons’ skin which is designed to stay there for the life of a person. A hand-held reader can access the information on the implanted microchip.

8) If a verification mark consisted of a microchip implanted by an injection under the skin similar to a vaccination needle then the physical process of getting a “mark” sounds easy.

SD				**SA**
❒	❒	❒	❒	❒

9) If a simple one-page form requiring your details together with appropriate proof of your identity was all that was administratively required to receive a “mark” then the administrative process of getting a “mark” sounds easy.

SD				**SA**
❒	❒	❒	❒	❒

10) If when a small scanner is waved over the “mark” information was accessible on the scanner screen via keyboard functions, it seems this would make it easy to retrieve information for example a monetary balance. (Consider in this answer and from now on that a password needs to be entered to access the “mark”).

SD **SA**

❒ ❒ ❒ ❒ ❒

11) If the “mark” was used to update monetary records instantly when receipts and payments are made via a scanner, which is linked to a global positioning satellite, then it seems easy to buy and sell.

SD **SA**

❒ ❒ ❒ ❒ ❒

12) If the procedure for a receipt or payment over the phone or computer was the same as what currently exists except a scanner is installed into the computers or phones to access the “mark” rather than keying in a card number then this seems easy. Note: the scanner would not distinguishably change the size or performance of the phones or computers and could be installed in a mobile phone.

SD **SA**

❒ ❒ ❒ ❒ ❒

13) If companies adopted a policy of authorised “marks” implanted into certain personnel then company transactions would be easy to record.

SD **SA**

❒ ❒ ❒ ❒ ❒

14) Please identify in order of importance up to four factors that you think might make a "mark" difficult to use

…….

……..…

……..…

…….

5.2.5 Perceived usefulness

The perception of usefulness also came from Davis' (1989) Technology Acceptance Model. The verification mark might be useful in both a private and business context. The survey examined perceived usefulness as shown in the following extract of each question from Section C: Usefulness of the survey.

Ling (2001) indicated that smart cards are being used as a substitute for cash. This research considered the potential of the "mark" replacing smart cards and the perceived usefulness of it is studied including accounting and taxation purposes. Murray (2002) acknowledged the achievement of real-time information update technology through Global Positioning Satellite. Question arose to examine the perceived usefulness of this advancement. There could be other potential factors not identified in the survey. An open question was included to provide an opportunity to gather qualitative information regarding the usefulness of the mark.

Question 15 deals with the usefulness of the "mark" in the area of accounting, and Question 16 deals with the usefulness of the "mark" in assisting the preparation of tax return as this would be an important function that affects the usefulness of the "mark". One major advantage of the mark is the real-time update function that facilitates the use of the mark to replace other cashless mediums of exchanges which has physical risks. Question 17 deals with the usefulness of the "mark" in replacing other mediums of exchange in the form of cards, and Question 18 deals with the usefulness of the "mark" in providing real-time identification. On the other hand, Question 19 was set up as an open question to collect the potential issues people presumed that make a "mark" useful.

Extract of questionnaire: Section C: Usefulness of the survey:

Your perceptions are being sought for the following questions on a scale from:

SD = Strongly Disagree to SA = Strongly Agree

Please tick the box that best fits with your reaction to each of the following statements.

15) If financial information stored via the "mark" could be downloaded into packages such as word or excel then this would make it useful in accounting for your personal transactions.

SD				**SA**
❒	❒	❒	❒	❒

6) A "mark" would be useful in collating information for your taxation return.

SD				**SA**
❒	❒	❒	❒	❒

17) A “mark” would be useful in reducing the burden of having to carry a card and or losing a card?

SD				SA
❒	❒	❒	❒	❒

18) If the person’s nationality, gender, medical and other relevant details were accessible on a real time basis via the “mark” and a scanner then this would be useful.

SD				SA
❒	❒	❒	❒	❒

19) Please identify up to four issues in order of importance that you think would make the verification mark useful in a private context?

……

……..……

……..……

…….

5.2.6 Risks

The technology acceptance model included perceived ease of use and perceived usefulness in the context of an organisation adopting a new computer environment. It could be argued that the element of risk was seen to have been borne by the organisation

rather than the user. A perceived risk element was included in the developed model given the context of this permanent and personal issue.

5.2.6.1 Potential for social control

Power asymmetry between the individual and the government, individual and the bank, and individual and the private organisation are imperative risks concerned using the "mark" (Rabinow, 1982). There could be other potential factors not identified in the survey. An open question was included to providing an opportunity to gather qualitative information on potential control risks.

The survey examined the potential implications of the "marks" used as social control as outlined in the extract of Part 1: Potential for social control.

If information is consolidated in such a substantial way the information may be used by powerful organisations such as governments, banks, or other private organisations in a way that may control a person's behaviour. Question 20-23 deals with the perceived government's/bank's/private organisation's control risks carried by the "mark" as this would be an important factor that some people may perceive to be risky. Question 24 being the open question was set up to collect the potential control risk factor that people maybe concerned about using the mark.

Extract of questionnaire: Part 1: Potential for social control.

20) A "mark" would increase the control

- The government have over my life in that they would be able to track all of my receipts and expenditures.

SD **SA**

❒ ❒ ❒ ❒ ❒

21)

- The government have over my life in that it would be able to track all of my affiliations and activities via my receipts and expenditures.

SD **SA**

❒ ❒ ❒ ❒ ❒

22)

- The banks have over my life.

SD **SA**

❒ ❒ ❒ ❒ ❒

23)

- Other private organizations have over my life.

	SD				SA
	❒	❒	❒	❒	❒

24) List in descending order up to four of your highest concerns relating to control over your life that a "mark" may bring

……

……

……

…….....

5.2.6.2 Privacy

As discussed in the literature review, privacy is one of the major issues arising from the use of the "mark" that most people maybe concerned about as a result of increased information available to them via the adoption of the "mark". Question 25-26 deals with the mitigation of privacy risks carried by the "mark" through legislation and constitution as this would be an important factors that affects people's risk perception an issue raised by Shaw (2005). Question 27 then examines people's perception or belief in whether the companies would act ethically and responsibly in dealing with privacy issues. The following is an extract of Part 2: Privacy of the survey.

Extract of questionnaire: Part 2: Privacy.

25) Carefully drafted changes to legislation designed to protect my privacy would indeed protect my privacy if the "mark" system were adopted.

SD				SA
❒	❒	❒	❒	❒

26) Carefully drafted changes to the constitution designed to protect my privacy would indeed protect my privacy if the "mark" system were adopted.

SD				SA
❒	❒	❒	❒	❒

27) I perceive companies will deal responsibly with privacy issues that would arise as a result of increased information available to them via the adoption of the "mark".

SD				SA
❒	❒	❒	❒	❒

5.2.6.3 Abuse

The survey examines risks which were considered by various authors including Moor (2002) who highlighted the importance to counter identity fraud and Barclay (2004) who addressed the issue of possible theft that might resulted from using the "mark". Perception on whether the implantable chip would help reduce the fraud or result in more fraud may affect the acceptance of the "mark".

The survey also considers the significance of what Van den Poel et al (1999) refers to as “risk relievers” (p. 254) and Roselius (1971) refers to as “risk reduction methods” (p. 56). Neiger (2002) examined the technology protection available against the abuse, raising the question of perception on technology controls protection.

Question 28 deals with the perceived risks of information abuse by companies as the potential risk of abuse resulting from increased information or power brought about by the “mark” is another important aspect of the risks. Question 29-30 considers risk of abuse in term of fraud and theft as this would be an important issue that affects the acceptance of the “mark”. Question 31 deals with technology control that helps prevent abuse as this would be an important issue that affects the perceived abuse risk of the “mark”. The following is an extract of Part 3: Abuse of survey.

Extract of questionnaire: Part 3: Abuse of survey.

28) I perceive companies will not abuse increased information or power brought about by the “mark”.

SD **SA**

❒ ❒ ❒ ❒ ❒

29) If a “mark” eventually eliminated the need for cash, cheques, credit cards and any other form of money outside barter then I perceive this would reduce the likelihood of

- fraud.

SD **SA**

❒ ❒ ❒ ❒ ❒

30)

- theft.

SD **SA**

❒ ❒ ❒ ❒ ❒

31) I perceive technology controls such as encryption software are capable of protecting me from abuse if the "mark" was adopted.

SD **SA**

❒ ❒ ❒ ❒ ❒

5.2.6.4 System corruption

The survey examines system corruption risks which were considered by various authors including Wenske (2003) who looked at risks in an online environment. The seriousness of a system collapse or virus could substantially affect the risk perception and thus the acceptance of the "mark". Question 32-33 deals with the perceived effects of a system corruption to be temporary/permanent. The following is an extract of Part 4: System corruption from survey.

Extract of questionnaire: Part 4: System corruption from survey.

32) I perceive a system collapse or virus

- could **temporarily** affect the official record of my financial position.

SD **SA**

❒ ❒ ❒ ❒ ❒

33)

- could **permanently** affect the official record of my financial position.

SD **SA**

❒ ❒ ❒ ❒ ❒

5.2.6.5 Other risks

Other risks have been considered informed by literature. Barclay (2004) addressed the issue of a potential foreign body reaction due to the implanting of a chip which was predicted to be less than 2 %. Lane (2003) also raised a concern about the long-term health effects of such devices transmitting signals from inside a person's body. The survey examines other risks in a closed question relating to health and provides the opportunity for respondents to contribute generally about other risks in an open question. The following is an extract of Part 5: Other risks from the survey.

Many people maybe concerned about the health and safety issue caused by chips implanted into the human body. Question 34 deals with the perceived risks in term of health and safety issues as this would be an important issue that affects the acceptance of the "mark". Question 35 was set up as the open question to collect potential risk factors of using the mark that are not considered in the closed questions.

Extract of questionnaire: Part 5: Other risks from the survey

34) I perceive a "mark" could affect my health or create a safety issue given that it would be implanted in my wrist or forehead.

SD **SA**

❒ ❒ ❒ ❒ ❒

35) Identify up to four other risks that you would associate with a "mark". List in descending order

…….

…….

…….

…….

5.2.7 Normative beliefs and motivation to comply

The survey explored the normative beliefs of the respondents. Michael et al (2005) indicated that religious advocates are concerned about the use of the information gathered and the functionality of the technology. A question (36) was asked to identify the affects influences of a religious nature has on the acceptance decision. Barclay (2004) discussed the community's resistance against the technology, driving the question about the affect the community's perception had on the acceptance decision resulting in Question 37. Ajzen and Fishbein (1980) included family members as one of the important groups who have influence over one's attitude. Respondee's perceptions about wether family members' attitudes towards the "mark" would be influential was asked (38). These questions were asked as representative of the most influential groups on a person's beliefs and behaviour. Question 39 being the open question was set up to identify the four most perceived influential groups of people. Question 40-42 investigates the perception of those influential groups on a "mark" becoming easy to use (Q40), useful (Q41), and risky (Q42). The following is an extract of Part E: Normative beliefs from the survey.

Extract of questionnaire: Part E: Normative beliefs

Your perceptions are being sought for the following questions on a scale from:

SD = Strongly Disagree to SA = Strongly Agree

Please tick the box that best fits with your reaction to each of the following statements.

36) A “mark” offends my religious beliefs.

SD				**SA**
❒	❒	❒	❒	❒

37) A “mark” conflicts with the views of my most influential community group.

SD				**SA**
❒	❒	❒	❒	❒

38) A “mark” conflicts with the views of my family.

SD				**SA**
❒	❒	❒	❒	❒

39) Identify four people or groups that you hold as important in your life in terms of the influence their opinions have on you, for example (religious institution, spouse, parents, children). List in descending order.

…...……

……..……

……..……

……

40) The person, people or groups that I hold as important to me would perceive that a "mark" was

- easy to use.

SD **SA**

❒ ❒ ❒ ❒ ❒

41)

- useful.

SD **SA**

❒ ❒ ❒ ❒ ❒

42)

- risky.

SD **SA**

❒ ❒ ❒ ❒ ❒

5.2.8 Pre-testing

Roberts (1999 p.73) stated that "criticisms of the survey method relating to the quality of data can be countered by the careful development of the instruments and questionnaires, by appropriate administration techniques". To this end the survey has been developed to collect data that provide both reliable and valid measures of the constructs. Whilst tests of consistency are used to identify the intentional falsification, pre-testing is done to minimize the bias resulted from unintentional mistake such as misunderstanding of the terms used in questionnaire.

A pre-testing was undertaken on 32 experienced and qualified professionals from three vocational groups (Young 2004). Eleven professionally qualified accountants were

selected, along with ten professionals from the information technology industry, who had the required experience and qualifications, and finally, eleven professionals with legal qualifications and work experience in the legal area. The professionals filled in all parts of the questionnaire with no evidence or communication of difficulty, which confirmed the effectiveness of the questionnaire and provided confidence on validity and overall survey quality.

The test of consistency of the questionnaire was analysed in the pre-test responses. For example, responses from the Likert style questions were tested to determine that Strongly Agreed labels and Strongly Disagree labels that communicated the same issue were filled in consistently by the respondents. The pre-testing supported the relationships established in the test of consistency and no inconsistencies were found.

5.3 Administration of the survey

The details of each accountant selected were transferred piece by piece into a Microsoft Office Excel file after attempts to download the data proved futile. A mail merge labelled the envelopes and an introductory letter, complete with appropriate protocol, the survey and a reply paid envelope were sent by post to all selected participants.

5.3.1 Survey response rate

The 523 surveys were sent on 1 December 2003. One Victorian practice was subsequently found to have closed leaving a total population of 522. There were 101 responses, a percentage of 19.35%. A second survey was sent on 23 February 2004 with an additional 66 replies a percentage of 12.65% accumulating to 167 replies, a percentage of 32%. Four of the replies were invalid and were removed as they ticked box 4 for question one, about professional affiliation, which meant they were not CPAs or CAs which was part of the requirements of the survey. 22 responses were not used in this part of the analysis as they failed to complete the closed part of the questionnaire. The open part of the questions was contributed to by these participants. This left 141 complete responses a percentage of 27%. If a participant did not fill in one or more closed question they were removed from the analysis in order to provide a very strict interpretation. A less rigorous approach could have led to a higher response rate. 15 participants had dual affiliations. Non responses bias was considered by modelling the early response and the late responses and comparing them with the model that included all of the responses. The detailed analysis has been included later in this research.

Table 5.7 Responses break down

Professional Body	State/territory	First Response	Second response	Total response
ICAA	NSW	12 –1=11 (2 CPA and ICAA)	7-3= 4	19-4=15
ICAA	Tasmania	0	0	0
ICAA	Northern Territory	1	0	1
ICAA	South Australia	3	1	4
ICAA	ACT	2 (2 CPA and ICAA)	0	2
ICAA	WA	2-1=1 (2 CPA and ICAA)	1	3-1=2
ICAA	Queensland	10-1=9 (3 CPA and ICAA)	2	12-1=11
ICAA	Victoria	6 –2 = 4 (1 CPA and ICAA)	6	12-2=10
CPA Australia	NSW	25-2=23 (4 CPA and ICAA)	11-2=9	36-4=32
CPA Australia	Tasmania	0	3-1=2	3-1=2
CPA Australia	Northern Territory	3	1	4
CPA Australia	South Australia	2	3	5
CPA Australia	ACT	1	2	3
CPA Australia	WA	1	4	5
CPA Australia	Queensland	11-2=9	7-1=6	18-3=15
CPA Australia	Victoria	22-3=19 (1 CPA and	18-3=15	40-6=34

		ICAA) (1 with no position detail)		
		101-12=89	66-10=56	167-22=145
Non professionals				4
				141
Dual affiliations			(15 CPA and ICAA)	

Statistical Package for Social Sciences version 14.0 (SPSS) was used to analyse the data. No response was found to have been in conflict with the communication of another response relating to the same issue. Other evidence also supported the fact that the survey was done in good faith, for instance, many took the time to fill in the open questions and the majority completed the survey in totality.

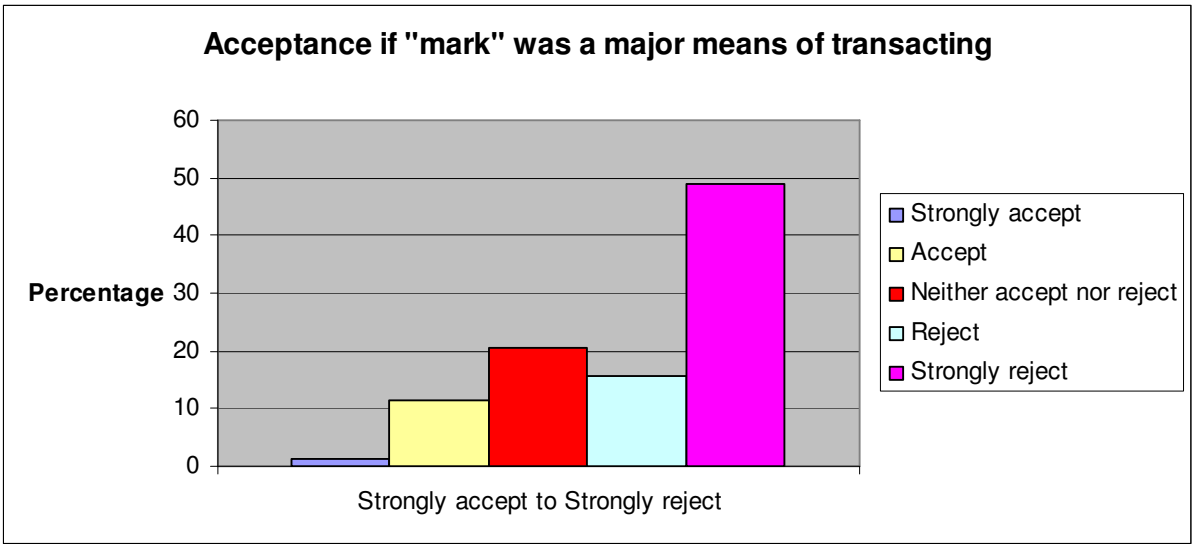
Chapter Six: Reporting and analysis of responses

The responses from the forty nine questions asked in the questionnaire were analysed and the outcomes are reported in this chapter. This chapter reported the analysis of the responses with the acceptance of the "mark", followed by the descriptive results. The responses were then analysed based on each of the four independent variables. Subsequently, the availability of technology was discussed and an analysis was undertaken on the validity of the research. Further, early and late response bias was examined and the hypotheses were tested. Finally, the chapter tested the technology acceptance model and examined the responses of open questions. Some charts, tables and graphs were provided in this chapter along with the analysis, not all of them are included in the content. Reference to Appendices is sometimes necessary.

6.1 Acceptance of the "mark"

The Graph 6.1 reflects that the dependent variable (acceptance of the mark if it "was a major means of transacting") was strongly accepted by 1% of the valid responses, accepted by 11% of the valid responses, rejected by 16% of the of the valid responses and strongly rejected by 49% of the valid responses. The number of valid responses was 141 (n = 141), the mean was 2 with a standard deviation of 1.14.

Graph 6.1 Acceptance if "mark" was a major means of transacting



6.1.1 Acceptance of the "mark" if it was compulsory

Table 6.1 details the perception of the respondents regarding the acceptance of the "mark" if it was compulsory.

Table 6.1 The percentage of acceptance if it was compulsory

Acceptance if it was compulsory	% Percent
Strongly Reject	68.1
Reject	12.1
Neutral	11.3
Accept	6.4
Strongly Accept	2.1
Total	100.0

6.1.2 Acceptance of the "mark" by groups

The perception of the respondents regarding the acceptance of the "mark" by groups who were important to them (refer to Appendix 1.41), was that no respondents perceived that groups who were important to them would strongly accept the "mark". 48% of the respondents perceived that the groups who are important to them would strongly reject the "mark", 5% of the respondents perceived that the groups who were important to them would accept the "mark' and 0% of the respondents perceived that the groups who were important to them would strongly accept the "mark". The result is in line with findings in 6.1 and 6.1.1.

6.2 Descriptive results

6.2.1 Professional membership and gender of respondents

Of the valid respondents (refer to Appendix 1.1) , 27% were members of the ICAA, 62% were members of CPA Australia and 11% were members of both bodies. Reconstructed member number details extracted from the CPA annual report (2000) and reported earlier in this research showed a ratio of 28% being members of the ICAA and 72% being members of CPA Australia. The similarity between the membership proportions of the respondees and the actual proportions of ICAA members to CPA members was to be expected as surveys were sent out in proportion to membership demographic. The number of respondents holding joint membership was surprising (around 11 %) and mainly came from the members initially identified as CPA members.

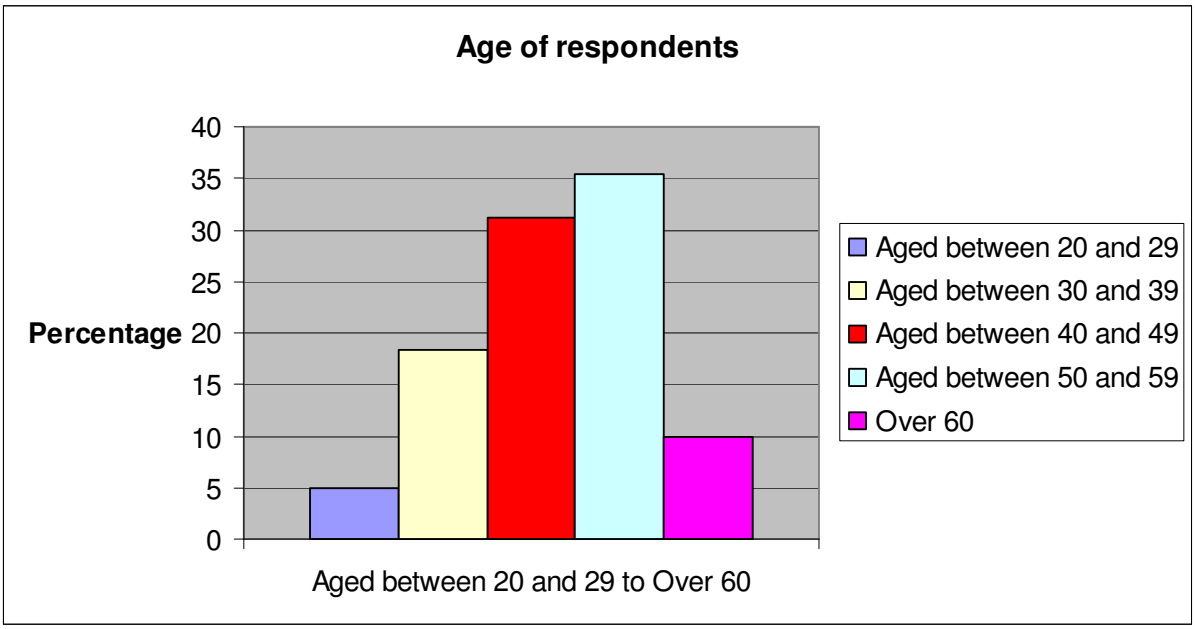
18.2% of the respondents were female which differs from the member demographics documented earlier in this research showing CPA members had a ratio of 49% females to 51% male in 2000. It was also noted earlier that the ICAA did not report this style of member detail. There were a greater number of males who were CPA members who responded to the survey. In preliminary tests to establish the importance of the various variables, a multinomial logit was run with "acceptance if the mark was a major means of transacting" as the dependent variable, with independent variables which included the elements of the model along with gender, age, profession, years in the profession, salary, position and field of employment. The only dependent variables that were significant when the multinomial logit was run were the elements of the model and this confirms the 'models' contribution. All of the other variables including gender were not significant. Therefore while there are some differences between the gender in the sample and the population, the difference does not affect the analysis because the gender variable is not significant.

6.2.2 Age of respondents

The following graph (Graph 6.2) is a reflection of the fact that 5% of the respondents were aged between 20 and 29, 18% were aged between 30 and 39, 31% were aged between 40 and 49, 36% were aged between 50 and 59 and 10% were aged above 60. This description shows that the respondents were weighted towards the 40 to 59 age groups. The number of valid responses was 141; the mean was 3.3 with a standard deviation of 1.03 implying that most responses came from experienced people. Member demographics reported earlier showed 18% of CPA Australia members were less than

30 years of age, 30% were between 30 and 39, 23% were between 40 and 49, 16% were between 50 and 59, 12% were over 60 years of age and 1% of member ages were unknown. Greater proportions of the respondents were aged from 50 to 59 years compared to the member demographics, arguably because of the survey focus on accounting practice owners. Younger members were less represented in the survey and it is argued that this is for the same reason.

Graph 6.2 Ages of respondents



6.2.3 Job position of respondents

66% of the respondents were partners, 5% were managers, 6% were seniors, 22% were assistants and 1% were in the "other" category. It can be seen the respondents were weighted towards being in more senior roles.

6.2.4 Salary of respondents

Table 6.2 Salary range of the respondents

Salary	% Percent
0-$30,000	5
$30,000-$60,000	15
$60,000-$100,000	38
Over $100,000	42
Total	100

It can be seen in Table 6.2, that the majority of the respondents were in the higher salary range. A person that receives a high salary often has proven themselves as having worth in their field of endeavour in this case financial services. That the majority of respondents to the survey had high salary could provide evidence that their input is valuable to research. One indicator of value is that the public are prepared to pay a high price for their input which has translated into a high salary for the professional.

6.2.5 Field of work of respondents

Table 6.3 shows the field of work undertaken by the respondents.

Table 6.3 Field of work of the respondents

Field of work	% Percent
Auditing	18
External reporting	2
Public sector	7
Finance	1
Information management and technology	1
Small business	37
Strategic business management	6
Superannuation	7

Taxation insolvency and reconstruction	14
Financial planning	1
Other	6
Total	100

It can be seen that the respondents have a wide variety of expertise within the accounting fields amongst them.

6.2.6 Numbers of years in the profession of the respondents

4% of the respondents had 5 or less years in the profession, 13% of the respondents had 6 to 10 years in the profession, 83% of the respondents had over 10 years in the profession. It can be seen that the contributions were weighted to more experienced accountants.

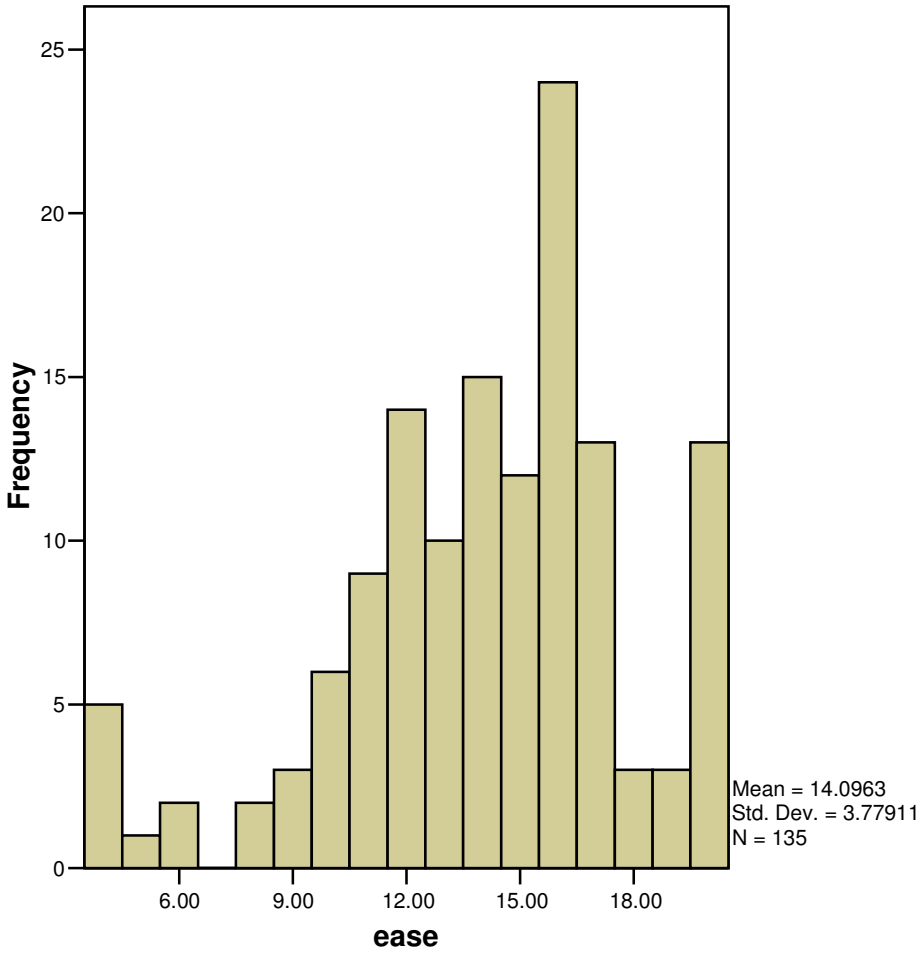
6.2.7 Descriptive information summary

The demographic information discussed in section 6.2.6 has shown that a large proportion of the respondents were experienced seniors and people who are likely to be decision and policy makers. The sample population fulfils the financial literacy test established in this research and is validated by the representativeness of the responses.

6.3 Ease of use

The respondents' contributions relating to ease of use are reflected below, first, as a whole (Graph 6.3) and second in Table 6.4 as individual components.

Graph 6.3 The respondent's contributions regarding ease of use



The graph shows a mean and skewness weighted towards the easy to use label. This is supported by Table 6.4.

Table 6.4 Ease questions' characteristics

Model	Kurtosis			Skewness		
Characteristics. Perceptions of:	Statistic	Standard error	Statistic/ Standard error	Statistic	Standard error	Statistic/ Standard error
Ease	0.607	0.422	1.43838863	-0.739	0.212	-3.48585

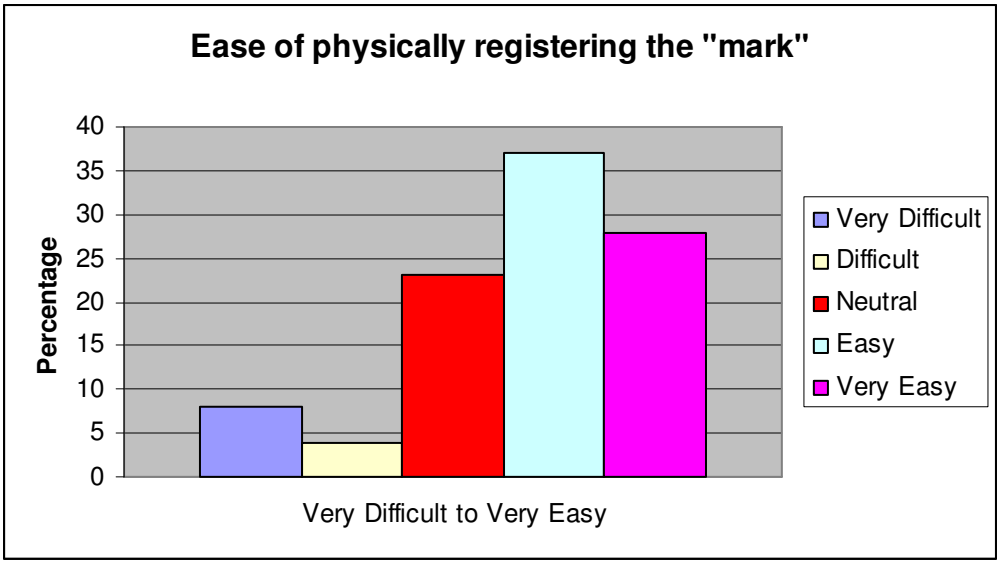
Overall, the responses to the "ease of use" questions were weighted towards the easy end as shown in Table 6.4. The negative skewness represents a weighting towards the easy side of responses (higher scores). There is some positive kurtosis in the ease of use

data indicating a more peaked distribution near the mean than normal data. This indicates responses tended to be around the indeterminate to easy label. The peak was pronounced at the easy label.

6.3.1 Ease of physical registration of the "mark"

The following bar graph (Graph 6.4) is a reflection of the fact that the perception of the respondents regarding the ease of the physical registration process were that 8% perceived it was very hard, 4% perceived it was hard, 37% perceived it was easy and 28% perceived the process was very easy. The number of valid responses was 141, the mean was 3.7 with a standard deviation of 1.15. It can be seen that the majority of the respondents felt that the physical side of registering the "mark" is either easy or very easy.

Graph 6.4 Ease of physically registering the "mark"



6.3.2 Ease of administratively registering the "mark"

Table 6.5 Easy administration registration percentage

Easy administration registration	% Percent
Very Hard	7
Hard	3
Neutral	18
Easy	46
Very Easy	26
Total	100

It can be seen in Table 6.5 that the majority of the respondents (46% and 26%) felt that the administration side of registering the "mark" is either easy or very easy.

6.3.3 Ease of access to information using the "mark"

The perceptions of the respondents regarding the ease of access to information using the "mark" (refer to Appendix 1.10) were that 5% perceived it was very hard, 4% perceived it was hard, 48% perceived it was easy and 21% perceived the process was very easy to access information using the "mark".

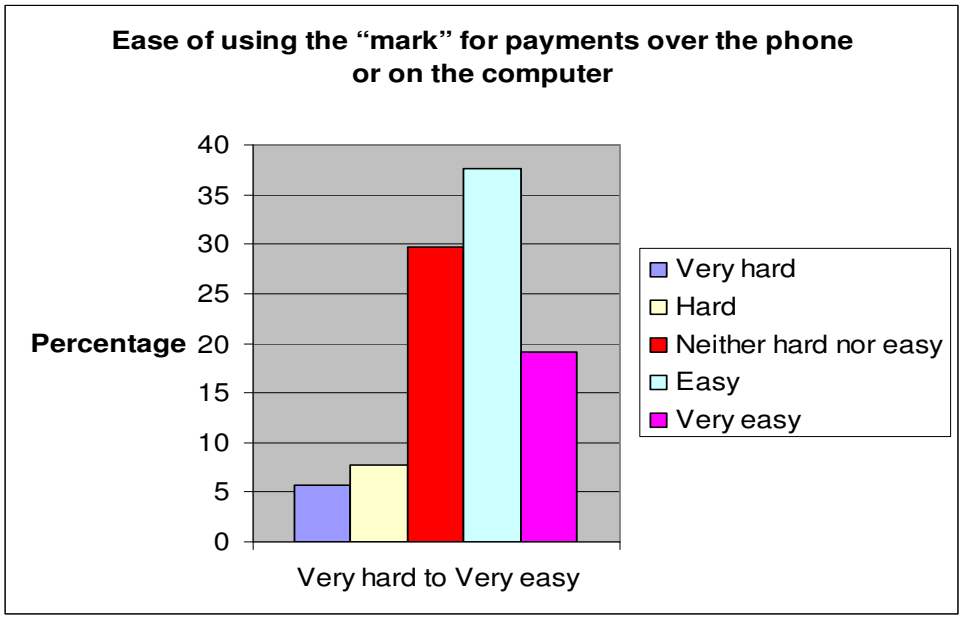
6.3.4 Ease of using the "mark" to buy and sell

The perception of the respondents regarding the ease of using the "mark" to buy and sell (refer to Appendix 1.11) was that 8% perceived the process was very hard, 9% perceived the process was hard, 36% perceived the process was easy and 18% perceived the process was very easy.

6.3.5 Ease of using the "mark" for payment over the phone or computer

The following bar graph (Graph 6.5) is a reflection that 6% of respondents, perceived making payments using the "mark" over the phone or on the computer was very hard, 8% perceived it would be hard, 38% perceived it was easy and 19% of the respondents perceived it would be very easy. The number of valid responses was 141, mean was 3.6 with a standard deviation of 1.06.

Graph 6.5 Ease of using the "mark" for payments over the phone or computer



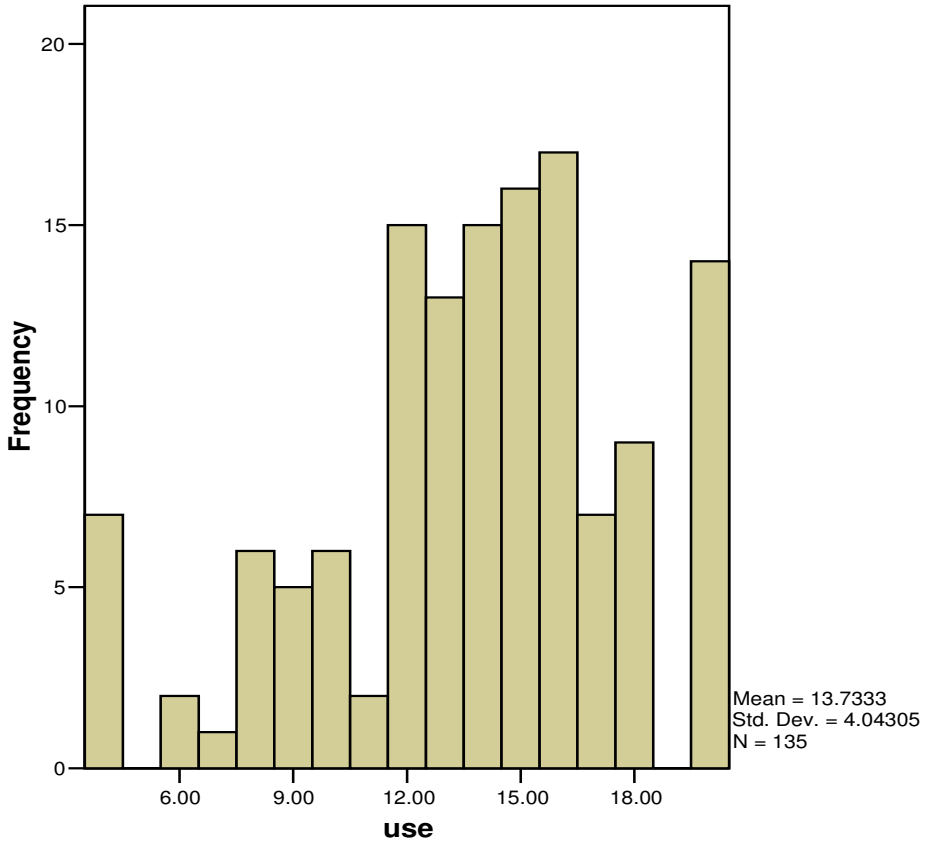
6.3.6 Ease of using the "mark" to create company records

The perceptions of the respondents regarding the ease of using the "mark" to create company records (refer to Appendix 1.13) were that 9% perceived it would be very hard, 12% perceived it would be hard, 40% perceived it would be easy and 14% felt it would be very easy.

6.4 Usefulness

The issues stated relating to the usefulness of the "mark" are reflected below first as a whole in Graph 6.6 and Table 6.6 then as individual components.

Graph 6.6 Usefulness of using "mark" – whole



The graph shows a mean and skewness weighted towards the useful label. This is supported by Table 6.6.

Table 6.6 Usefulness questions' characteristics

Model	Kurtosis			Skewness		
Characteristics. Perceptions of:	Statistic	Standard error	Statistic/ Standard error	Statistic	Standard error	Statistic/ Standard error
Useful	-0.721	0.42	-1.7166667	-0.502	0.212	-2.36792

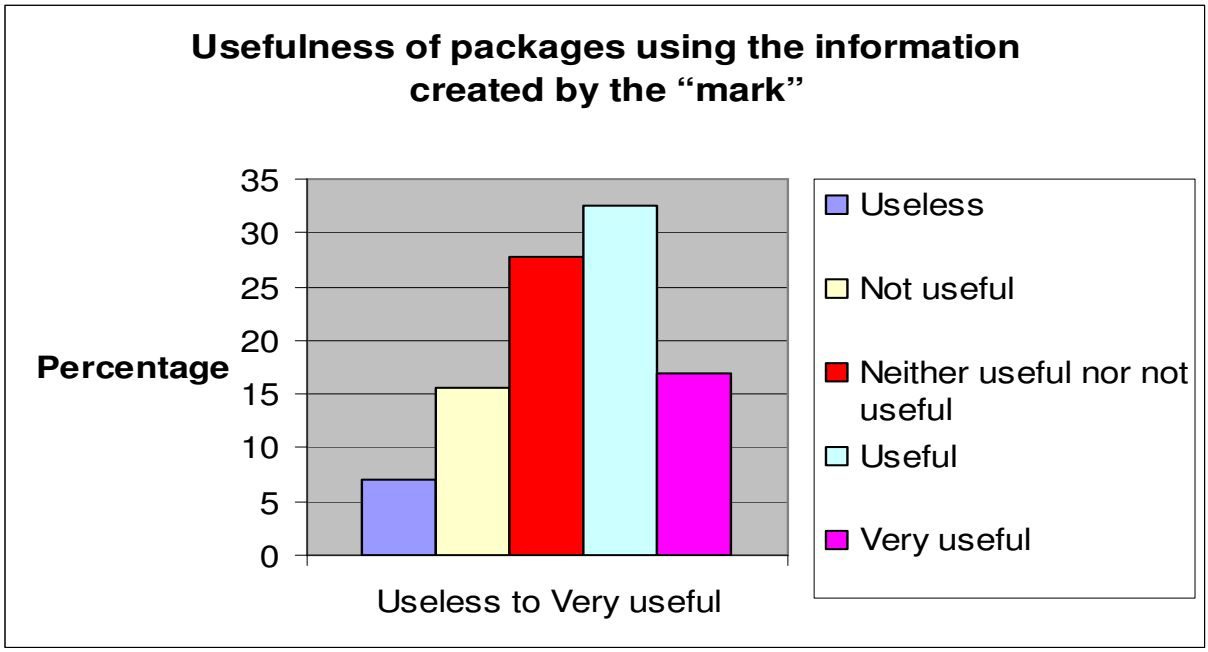
Overall, the responses to the "usefulness" questions were weighted towards the useful end as shown in Table 6.6. The negative skewness represents a weighting towards the useful side of responses (high scores). There is some negative kurtosis in the usefulness

data indicating a flatter distribution near the mean than normal data. This indicates responses tended to be around the indeterminate to useful label.

6.4.1 Usefulness of packages using the information created by the "mark"

Graph 6.7 reflects the perception of the respondents regarding the perceived usefulness of packages using the information created by the "mark". The results were that 7% of the respondents perceived that the packages would be useless, 16% perceived they would not be useful, 32% perceived that would be useful and 17% of the respondents perceived that the packages would be very useful. The number of valid responses was 141, mean was 3.4 with a standard deviation of 1.15.

Graph 6.7 Usefulness of packages using the information created by the "mark"



6.4.2 Usefulness of taxation information created by the "mark"

Table 6.7 details the perception of the respondents regarding the usefulness of taxation information created by the "mark". The majority of respondents (28%) perceived the use of the "mark" would provide useful taxation information and 29% of respondents took a neutral position.

Table 6.7 The percentage of useful taxation information

Useful taxation information	**% Percent**
Useless	12
Not Useful	16
Neutral	29
Useful	28
Very Useful	15
Total	100

6.4.3 Usefulness of not needing cards because of the "mark"

The perception of the respondents regarding the usefulness of not needing cards because of the "mark" (refer to Appendix 1.16) were that 10% of the respondents perceived it would be useless, 9% perceived it would not be useful, 30% perceived it would be useful and 31% perceived it would be very useful.

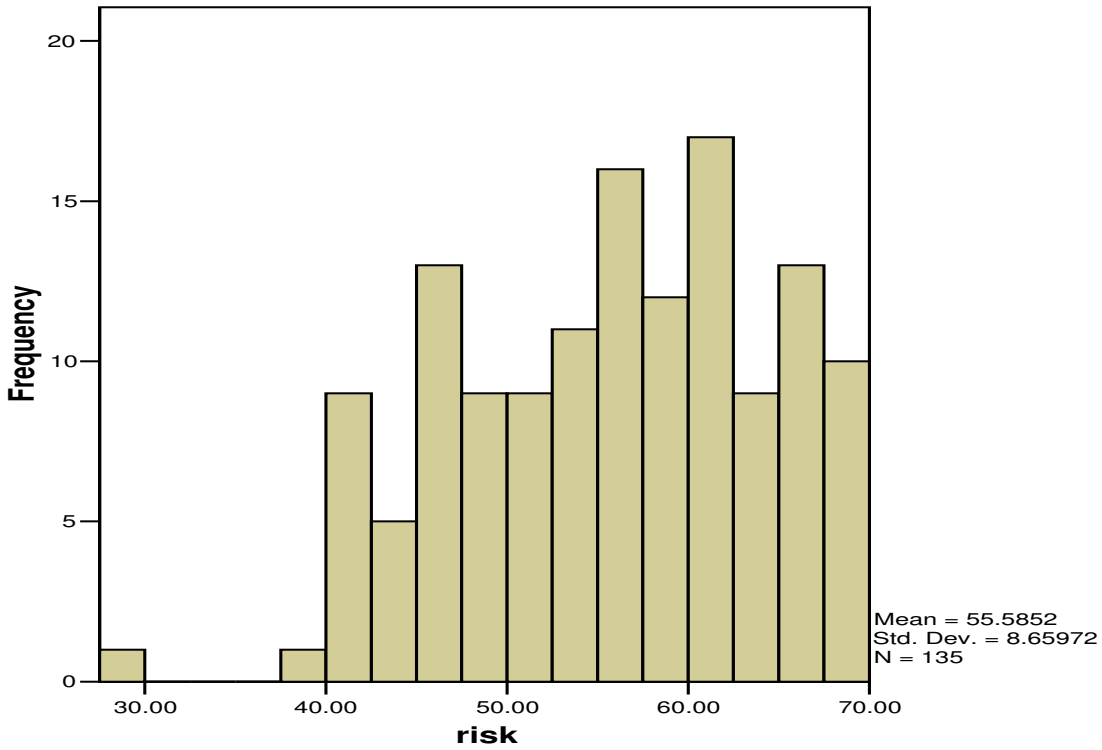
6.4.4 Usefulness of not having to carry medical and other information because of the "mark"

Having an implantable chip has the potential to store other information including medical information. The perception of the respondents regarding the usefulness of not having to carry medical and other information on the "mark" (refer to Appendix 1.17) were that 9% of the respondents perceived that it would be useless, 9% perceived it would not be useful, 37% perceived it would be useful and 24% perceived it would be very useful.

6.5 Risk of the "mark"

The contributions relating to the risks of the "mark" are reflected below, first as a whole in Graph 6.8 and then Table 6.7 then as individual components.

Graph 6.8 Risk questions' characteristics



Graph 6.8 shows a mean and skewness weighted towards the risky label. This is supported by Table 6.7.

Table 6.8 Risk questions' characteristics

The characteristics for the risk questions are identified below.

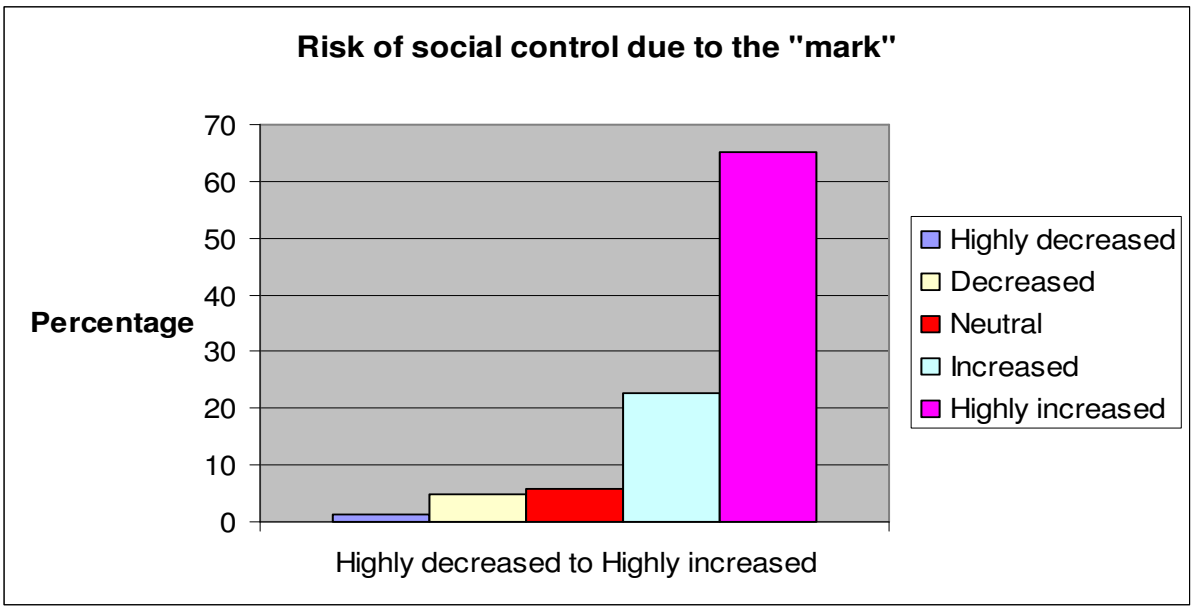
Model	Kurtosis			Skewness		
Characteristics. Perceptions of:	Statistic	Standard error	Statistic/ Standard error	Statistic	Standard error	Statistic/ Standard error
Risk	-0.435	0.428	-1.0163551	-0.39	0.216	-1.80556

Overall, the responses to the "risk" questions were weighted towards the risky end as shown in Table 6.8. The negative skewness represents a weighting towards the risky side of responses (higher scores). There is some negative kurtosis in the risky data indicating a flatter distribution near the mean than normal data. Responses tended to be around the indeterminate to risky and very risky labels.

6.5.1 Risk of social control due to the “mark”

Graph 6.9 reflects the perception of the respondents regarding the perceived risk of social control due to the “mark”. The results showed that 1% of the respondent felt that social control would highly decrease, 5% felt it would decrease, 23% felt it would increase and 65% felt it would highly increase. The number of valid responses was 141, the scale mean was 4.5 with a standard deviation of 0.91.

Graph 6.9 Risk of social control due to the “mark”



6.5.2 Risk of government control due to the “mark”

Table 6.9 details the perception of the respondents regarding the risk of government control via affiliations due to the “mark”. The results showed that 1% of the respondent perceived the risk would highly decrease, 5% perceived it would decrease, 18% felt it would increase and 67% felt it would highly increase.

Table 6.9 Risk of government control due to the "mark"

Risk of government social control via affiliations due to the "mark"	% Percent
Highly decreased	1
Decreased	5
Neutral	9
Increased	18
Highly increased	67
Total	100

6.5.3 Risk of bank control due to the "mark"

The perception of the respondents regarding the risk of bank control due to the "mark" (refer to Appendix 1.20) were that 2% of the respondents felt bank control would be highly decreased, 9% of the respondents felt bank control would be decreased, 24% felt bank control would be increased and 54% felt bank control would be highly increased.

6.5.4 Risk of private organisation control due to the "mark"

Table 6.10 details the perception of the respondents regarding the risk of private organisation control due to the "mark". The results showed that 3% of the respondent felt that the risk would highly decrease, 8% felt it would decrease, 21% felt it would increase and 55% felt it would highly increase.

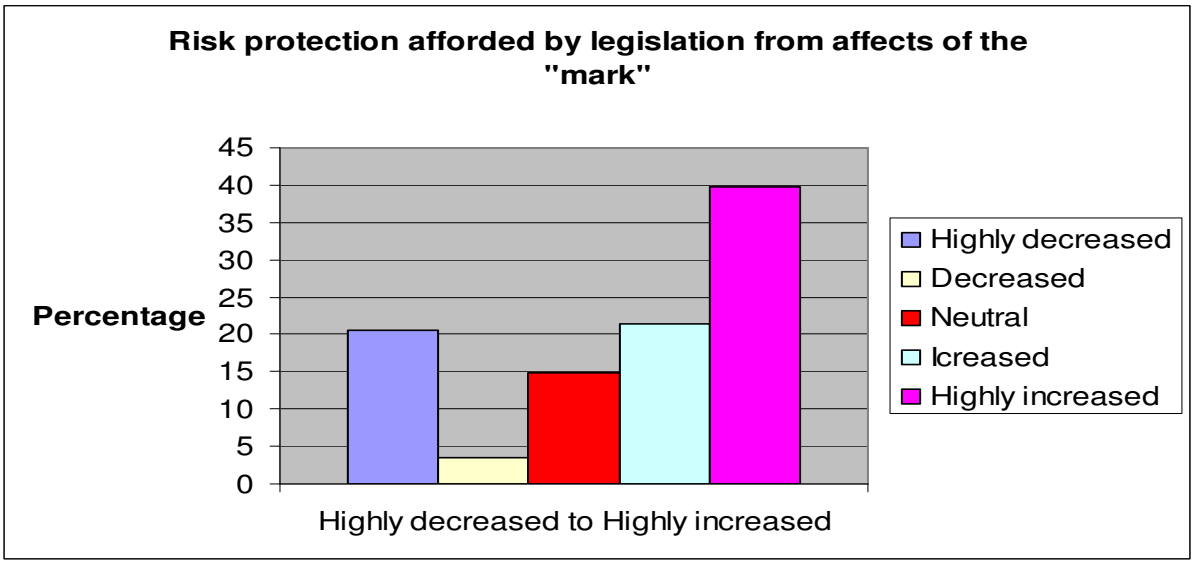
Table 6.10 Risk of private organisation control due to the "mark"

Risk of private organisation control	% Percent
Highly decreased	3
Decreased	8
Neutral	13
Increased	21
Highly increased	55
Total	100

6.5.5 Legislative protection against risks that may occur because of the "mark"

Graph 6.10 reflects the perception of the respondents regarding the perceived amount of risk protection that legislation would afford against any risks that would be caused by having the implanted chip. The results showed that 21% of respondents perceived risk protection would be highly decreased, 4% of the respondents perceived it would be decreased, 21% of the respondents perceived it would be increased and 40% perceived risk protection would be highly increased. The number of valid responses was 141, the mean was 3.6 with a standard deviation of 1.54

Graph 6.10 Risk protection afforded by legislation from affects of the "mark"



6.5.6 Constitutional protection against risks that may occur because of the "mark"

The perception of the respondents regarding the risk protection the constitution would afford against any risks that occurred due to the implanting of the chip (refer to Appendix 1.23) were that 14% of the respondents felt risk protection would be highly decreased, 6% felt risk protection would be decreased, 21% felt risk protection would be increased and 43% felt risk protection would be highly increased.

6.5.7 Risk of privacy loss due to companies receiving additional information because of the "mark"

Table 6.11 details the perception of the respondents regarding the risk of lost privacy due to companies receiving additional information because of the "mark". The results showed that 3% of the respondent felt that the risk of privacy from companies would highly decrease, 8% felt it would decrease, 23% felt it would increase and 54% felt it would highly increase.

Table 6.11 The percentage of risk of privacy from companies

Risk of privacy from companies	% Percent
Highly decreased	3
Decreased	8
Neutral	12
Increased	23
Highly increased	54
Total	100

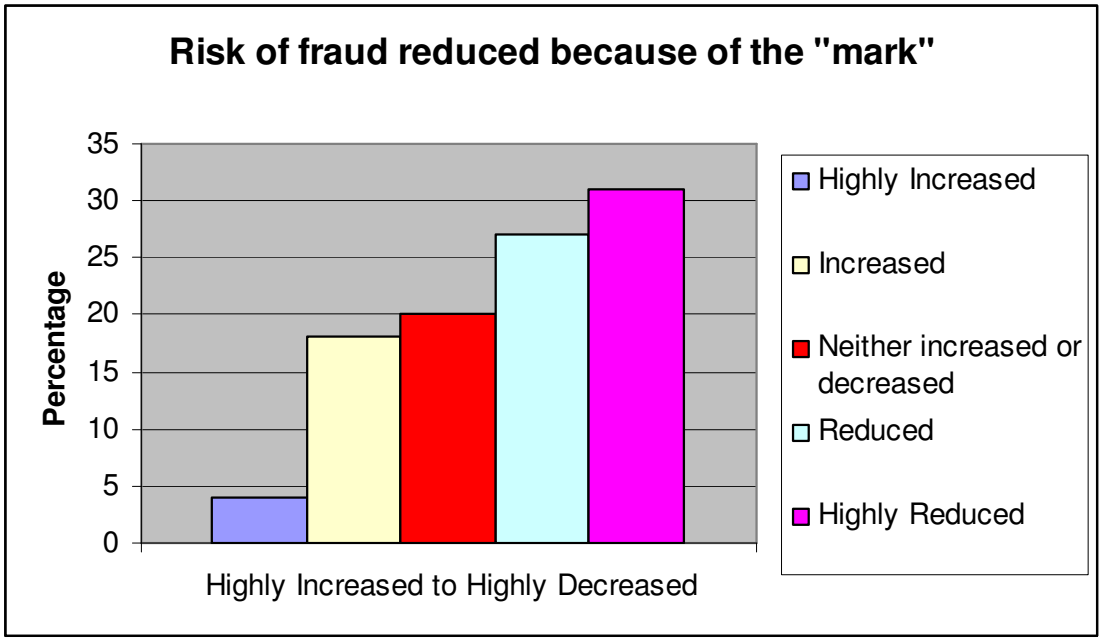
6.5.8 Risk of abuse from companies due to the "mark"

The perception of the respondents regarding the risk of abuse from companies due to the "mark" (refer to Appendix 1.25) were that 4% of the respondents perceived that the risk of abuse would be highly decreased, 6% of the respondents felt risk of abuse would be decreased, 29% felt the risk of abuse would be increased and 54% felt the risks would be highly increased.

6.5.9 Risk of fraud reduced due to having the “mark”

Graph 6.11 below identifies the perception of the respondents regarding the risk of fraud being reduced by having the implanted chip. The results showed that 4% of respondents perceived the risk of fraud would be highly increased, 18% of the respondents perceived the risk of fraud would be increased, 27% of the respondents perceived the risk of fraud would be reduced and 31% perceived the risk of fraud would be highly reduced. The number of valid responses was 141, the mean was 3.6 with a standard deviation of 1.22.

Graph 6.11 Risk of fraud reduced because of the “mark”



6.5.10 Risk of theft reduced because of the "mark"

The perception of the respondents regarding the risk of theft reduction because of the "mark" (refer to Appendix 1.27) were that 7% of the respondents perceived that theft would be highly increased, 16% of respondents felt theft would be increased, 23% perceived theft would be reduced and 31% of the respondents perceived theft would be highly reduced.

6.5.11 Risk of the "mark" reduced because of software encryption

The perception of the respondents regarding whether risks of having the "mark" would be reduced by software encryption (refer to Appendix 1.28) were that 1% of respondents felt the risks would be highly increased, 11% felt the risks would be increased, 26% of the respondents would be reduced and 43% of the respondents felt it would be highly reduced.

6.5.12 Risk of temporary corruption because of the "mark"

Table 6.12 details the perception of the respondents regarding the risks of temporary corruption because of the "mark".

Table 6.12 The percentage of risks for temporary corruption

Risks of temporary corruption	% Percent
Very low	5
Low	4
Neutral	6
High	40
Very High	45
Total	100

6.5.13 Risk of permanent corruption because of the "mark"

The perceptions of the respondents regarding the risk of permanent corruption of the information gathered by the "mark' were that 5% of the respondents felt strongly that the risk of permanent corruption was very low with a "mark", 5% of respondents felt that the risk was low, 25% of the respondents felt that the risk was high and 40% of the respondents felt that the risk was very high.

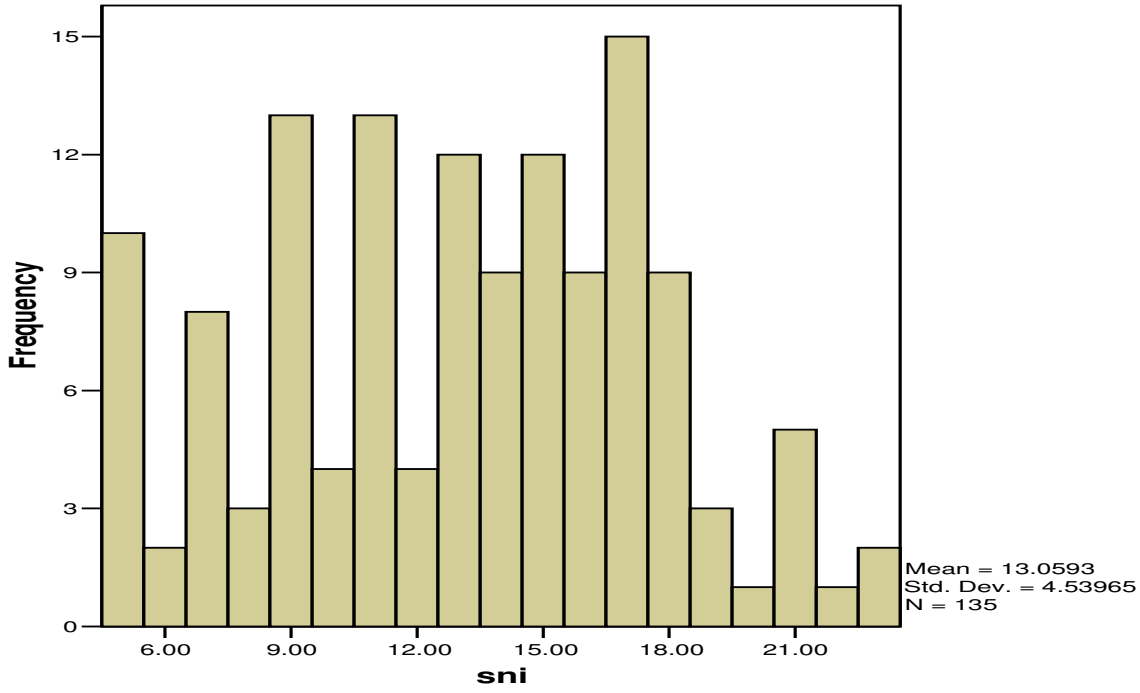
6.5.14 Risk of health issues because of the "mark"

The perceptions of the respondents regarding the risk of health issues (refer to Appendix 1.31) were that 6% of respondents felt that it was very unlikely the "mark" would adversely affect health, 16% of the respondents felt it was unlikely that the "mark" would adversely affect health, 23% of respondents felt it was likely that the "mark" would affect health and 20% felt it was highly likely that the "mark" would affect health.

6.6 Subjective norm

The views expressed relating to the subjective norm relating to the "mark" are reflected below; first as a whole in Graph 6.12 and Table 6.12 then as individual components.

Graph 6.12 Subjective Norm Frequency



Graph 6.12 shows a mean and skewness weighted towards a lack of support from those important to the respondents. This is supported by Table 6.12.

Table 6.13 Subjective norm questions' characteristics

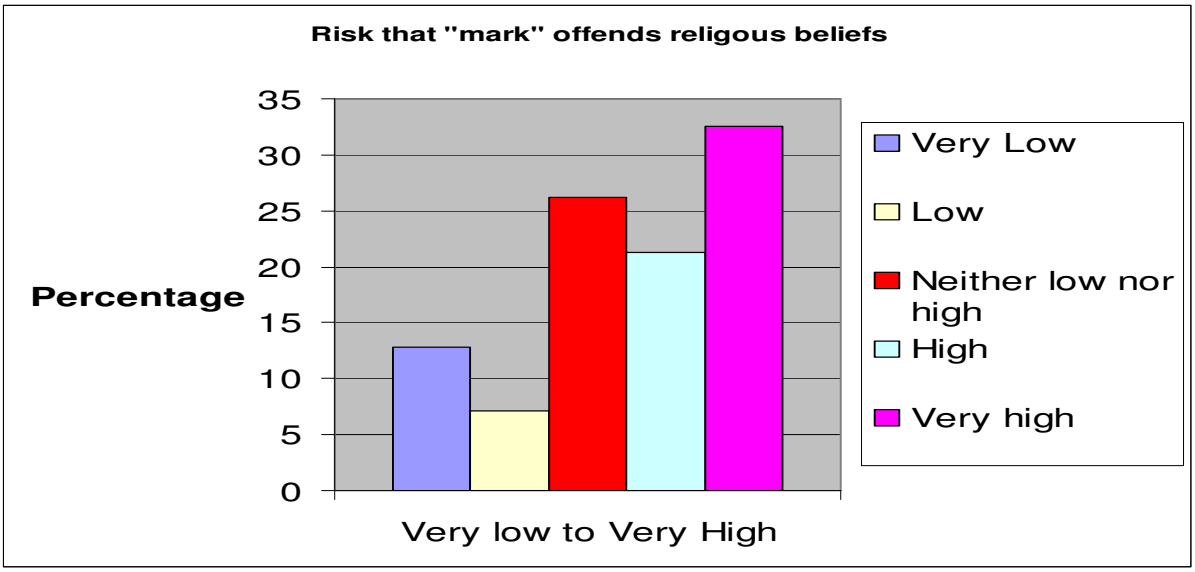
Model	Kurtosis			Skewness		
Characteristics. Perceptions of:	Statistic	Standard error	Statistic or Standard error	Statistic	Standard error	Statistic or Standard error
Normative beliefs	-0.449	0.428	-1.0490654	0.327	0.216	1.513889

Overall, the responses to the subjective norm questions were weighted towards the lack of support end as shown in table 6.13. The positive skewness represents a weighting towards the lack of support side of responses (high scores). There is some negative kurtosis in the subjective norm data indicating a flatter distribution near the mean than normal data. Responses tended to be away from the strongly support label.

6.6.1 Perception regarding the risk of the "mark" offending respondents' religious beliefs

Graph 6.13 details the perception of the respondents regarding the risk of offending their religious beliefs. 13% of respondents very strongly believed the "mark" did not offend their religious beliefs, 7% believed the "mark" did not offend their religious beliefs, 21% strongly believed the "mark" did offend their religious beliefs and 32% very strongly believed the "mark" did offend their religious beliefs. The number of valid responses was 141, the mean was 3.5 with a standard deviation of 1.35.

Graph 6.13 Risk that "mark" offends religious beliefs



6.6.2 Risk of the "mark" offending community groups

Table 6.14 details the perception of the respondents regarding the risks of offending community groups. The results showed that 17% of the respondents felt it is not risky that the "mark" would offend community groups, 11% felt it is not very risky, 22% felt it is risky and 16% felt it is very risky.

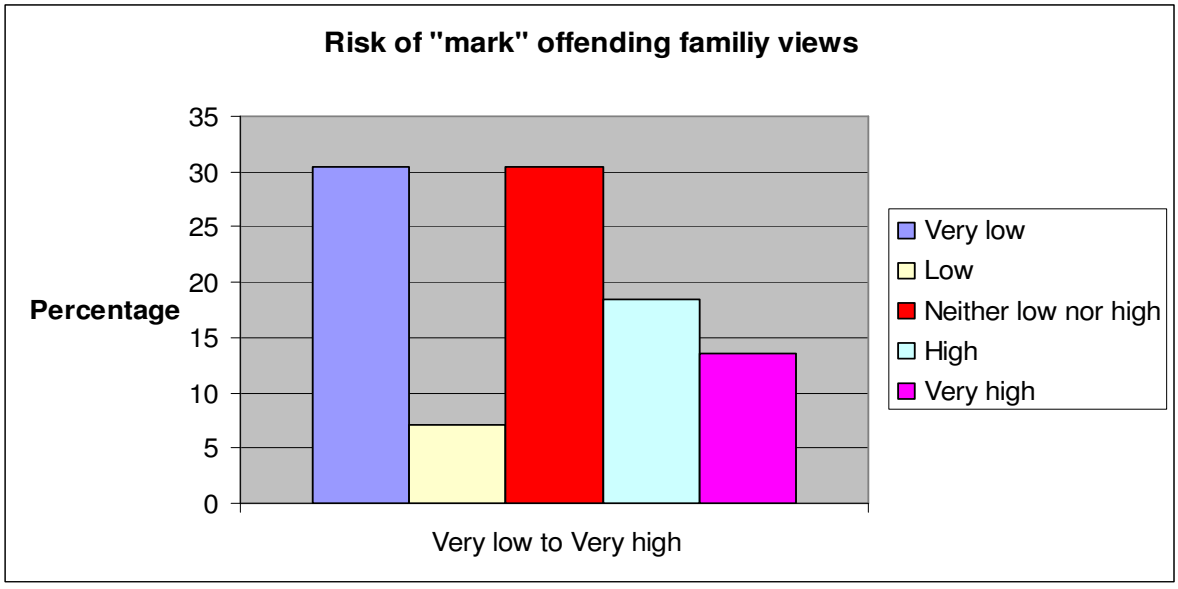
Table 6.14 The percentage for risks of offending community groups

Risks of offending community groups	% Percent
Not risky	17
Not Very Risky	11
Neutral	34
Risky	22
Very Risky	16
Not risky	100

6.6.3 Perception regarding the risk of the "mark" offending respondents' family views

Graph 6.14 details the perception of the respondents regarding the risk of offending their family views. 31% very strongly believed the "mark" did not offend their family views, 7% strongly believed the "mark" did not offend their family views, 18% strongly believed the "mark" did offend their family views and 14% very strongly believed the "mark" offended their family views. The number of valid responses was 141, the mean was 2.8 with a standard deviation of 1.41.

Graph 6.14 Risks of "mark" offending family views



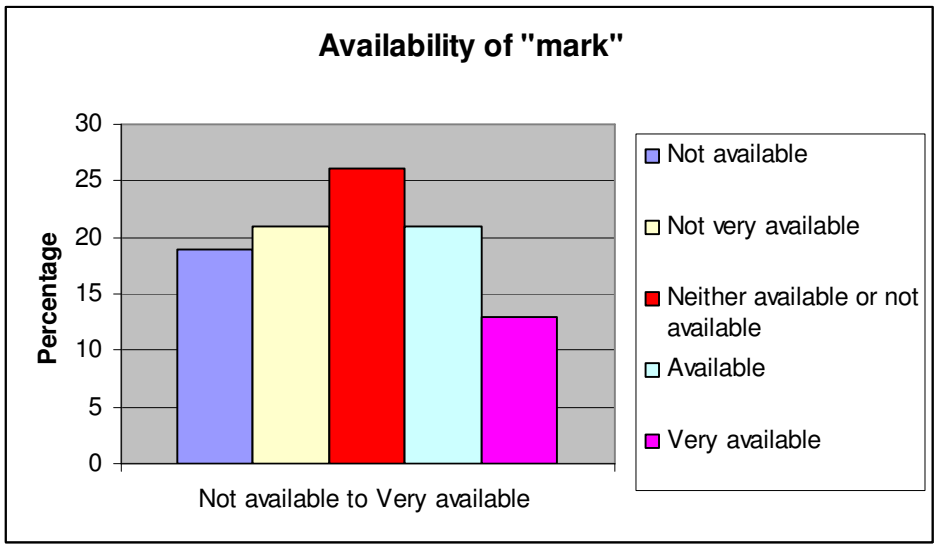
6.7 Availability of technology

Questions were asked to determine whether the respondents believed the technology detailed in the survey was currently available. The questions were asked in several stages and are referred to in the following paragraphs.

6.7.1 Availability of the implantable chip (mark) technology

Questions were asked to determine whether the respondents believed the implantable chip technology detailed in the survey were currently available. Graph 6.15 details the perception of the respondents. The results showed 19% of the respondents very strongly believed the implantable chip technology was not available, 21% of the respondents strongly believed the implantable chip technology was not available, 21% strongly believed the implantable chip technology was available and 13% very strongly believed the implantable chip technology was available. The number of valid responses was 141; the mean was 2.9 with a standard deviation of 1.30.

Graph 6.15 Availability of "mark"



6.7.2 Availability of technology surrounding the "mark"

Table 6.15 details the perception of the respondents regarding whether the technology surrounding the implantable chip (mark) allowing a cashless monetary system is available. The results showed that 12% of the respondent perceived that the other technology would not be available, 14% perceived it would not be very available, 34% perceived it would be available and 17% perceived it would be very available.

Table 6.15 The percent of the other technology is available

The other technology is available	**% Percent**
Not Available	12
Not Very Available	14
Neutral	23
Available	34
Very Available	17
Total	100

6.7.3 Availability of combined technology

The perception of the respondents regarding whether the combined "mark" technology (refer to Appendix 1.40) was available were that 12% very strongly believed the technology was not available, 22% strongly believed the technology was not available, 22% strongly believed the technology was available and 14% strongly believed the technology was available.

6.8 Validity of research

The survey questionnaire using a 5-point Likert scale was designed to solicit views on the various elements of the model. How well these questions that were grouped together and actually load as a factor, is important to determine whether it is reasonable to add the questions into one variable.

6.8.1 Cronbach's alpha

To test reliability, Cronbach's alpha was used, which is "a measure of internal reliability used in the evaluation of Likert scales" (de Vaus 2002 p.358). The results are displayed in Table 6.16. This Table shows that perceived ease of use had six items (Questions 8, 9, 10, 11, 12, 13) loaded as a factor with an alpha of 0.9140, which is well above the deemed acceptability rating of 0.7 (de Vaus 2002 p.184). Perceived usefulness had four items (Questions 15, 16, 17, 18) loaded as a factor with an alpha of 0.8670, which is well above the deemed acceptability rating. Perceived risk had fourteen items (Questions 20, 21, 22, 23, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34) loaded as a factor with an alpha of 0.8151which is well above the deemed acceptability. Perceived subjective norm had five (Questions 36, 37, 38, 42, 46) loaded as a factor with an alpha of 0.8058 which is well above the deemed acceptability rating.

Table 6.16 Cronbach's alpha for respondents' contribution

Elements	Items	Alpha
Perceived ease of use	Six (Questions 8, 9, 10, 11, 12, 13)	0.9140
Perceived usefulness	Four (Questions 15, 16, 17, 18)	0.8670
Perceived risk	Fourteen (Questions 20, 21, 22, 23, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34.)	0.8151
Perceived subjective norm	Five (Questions 36, 37, 38, 42, 46)	0.8058

The results showed support for using the grouped questions as a scale variable with all elements of the model achieving an alpha well above the deemed acceptability rating of 0.7 (de Vaus 2002 p. 184).

6.8.2 Multi-colinearity

It is also important to determine whether multi-colinearity exists, that is, if the explanatory variables are related to one another. If they are, then the factors can be confused making it impossible to get their independent effect on the dependent variable. The results are displayed in Table 6.17.

Table 6.17 Tolerance and VIF

Constant	Tolerance	VIF
EASE	.498	2.008
RISK	.669	1.494
SNI	.695	1.439
USE	.481	2.078

It can be seen that the "Tolerance" for each element of the model is greater than 0.1 showing that there is not a high degree of interrelationship between the factors supporting the importance of each group for the prediction of acceptance (Systat 1999 p. 380). The VIF statistic also shows that there is not a high degree of interrelationship between the factors supporting the importance of each group for the prediction of acceptance differently as it is less than 10. The VIF is the inverse of the tolerance.

6.8.3 Factor analysis

A factor analysis was undertaken to check if the items loaded on to the same variables as the model. A rotated component matrix was used as the relationships of the acceptance decision can be more clearly seen. The results are displayed in Table 6.18 with loading less than 0.4 in magnitude suppressed to improve the clarity of the presentation.

Table 6.18

Rotated Component Matrix(a)

	Component						
	1	2	3	4	5	6	7
8 Easy physical registration	.658						
9 Easy administration registration	.806						
10 Easy access	.848						
11 East to buy and sell	.869						
12 Easy payment over phone or computer	.844						
13 Easy company records	.821						
16 Useful taxation information	.640				-.401		
15 Useful packages	.766						
17 Useful not having cards	.648						
18 Useful having medical information	.635						
20 Risk of social control		.873					
21 Risk of government control		.877					
22 Risk of bank control		.831					
23 Risk of private organization control		.848					
25 Risk protection from legislation						.910	
26 Risk protection from the constitution						.874	
27 Risk of privacy from companies					.739		
28 Risk of abuse from companies					.764		
29 Risk of fraud reduced				.911			
30 Risk of theft reduced				.930			
31 Risks reduced by software encryption				.461	.474		
32 Risks of temporary corruption							.837
33 Risks of permanent corruption							.629
34 Risks of health issues			-.510				
36 Risks of offending religious groups			.785				
37 Risks of offending community groups			.800				
38 Risks of conflicting with family views			.804				
42 Groups find it useful			.559				
46 Acceptance by groups			.485		-.410		

(Extraction Method: Principal Component Analysis. Rotation Method: Varimax with Kaiser Normalization.
a Rotation converged in 7 iterations.)

The Rotated Component Matrix had a high loading for all of the perceived ease of use and perceived usefulness questions and loaded them on one factor. The modified Technology Acceptance Model had these separated in consideration of the contributions

of Davis' (1989) Technology Acceptance Model. Davis' (1989) model had perceived ease of use and perceived usefulness as two separate labels. All subjective norm questions clustered and had high loadings, which showed them up as a factor supporting its inclusion in the modified model.

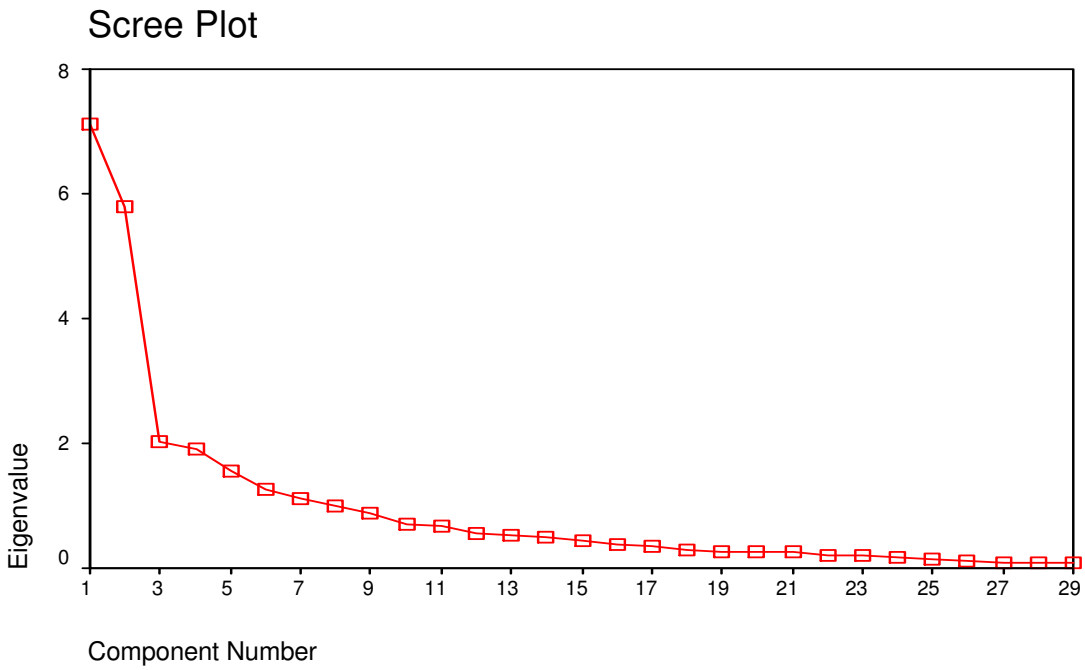
This result supports the introduction of risk as an element of the modified Technology Acceptance Model. The rotated component matrix had two risk factors. More specifically, the styles of potential risks showed up as a factor as did the risk mitigation questions. The model copes with the two risk factors by offsetting the perceived risks with the perception of mitigated risks. For example, if respondent felt privacy was at risk with the mark and that legislation could reduce the risk, then this was represented as a lower risk than had legislation not been seen as a means of mitigating the risk.

6.8.4 Scree plot

The Scree plot Graph 6.16 using Eigen values shows the incremental contributions that the factors are making to the explanation of the dependent variable. It is clear that the first four factors make valuable contributions after which the graph levels off. The first four factors are:

1. Ease of use and usefulness (7.2)
2. Risk of control (5.8)
3. Subjective norms (2.1)
4. Risk mitigation (1.9)

Graph 6.16



6.9 Multinomial Logits

The Multinominal logit model was used, as the dependent variable was determined using a survey with a five point Likert scale. The restriction of opportunity to differentiate responses with the five-point scale meant the data fundamentally retained the nature of ordinal data.

6.9.1 Multinominal logit modelling testing for late response bias

Early respondees were considered to be those who responded to the first survey. Late responses were those that responded to the second mail out of the survey. The late

responses were received between March and May. The first responses were coded as zero in SPSS to reflect time period 0 and the late responses were coded as 1 or time period 1. The results displayed in Table 6.19 show that there is an indication of some differences between early and late responders.

Table 6.19

Descriptive Statistics (a)

RESPONSE		N	Minimum	Maximum	Mean	Std. Deviation
Early	USE	83	4.00	20.00	14.4699	3.76873
	EASE	83	4.00	20.00	14.5301	3.46529
	RISK	83	28.00	70.00	54.8554	8.73196
	SNI	83	5.00	23.00	13.2530	4.59279
	Valid N (list wise)	83				
Late	USE	58	4.00	20.00	12.7414	4.40717
	EASE	58	4.00	20.00	13.6207	4.12024
	RISK	58	38.00	70.00	56.4483	8.92497
	SNI	58	5.00	21.00	12.7931	4.49076
	Valid N (list wise)	58				

6.9.2 Early response

As there were indications of response bias as seen in Table 6.19, the Multinomial Logit model was estimated for the early and late responses separately. The model using only early responses is significant, as seen in Table 6.20.

Table 6.20

Model Fitting Information

Model	-2 Log Likelihood	Chi-Square	df	Sig.
Intercept Only	122.946			
Final	61.206	61.740	12	.000

We can see in Table 6.21, that Perception of Subjective Norm (SNI) and Perception of Usefulness (USE) are both significant in explaining the dependent variable at the 95% confidence level (significances of 0.000 and 0.000 respectively). Perception of risk (RISK), and Perception of Ease of Use (EASE) were not proven to be significant for early respondees (significances of 0.535 and 0.098 respectively).

Table 6.21

Likelihood Ratio Tests

Effect	-2 Log Likelihood of Reduced Model	Chi-Square	Df	Sig.
Intercept	74.390	13.183	3	.004
EASE	67.499	6.293	3	.098
RISK	63.392	2.186	3	.535
SNI	90.505	29.298	3	.000
USE	88.589	27.382	3	.000

6.9.3 Late response

As can be seen in Table 6.22, the model using the late responses was also seen as significant with a 0.000.

Table 6.22

Model Fitting Information

Model	-2 Log Likelihood	Chi-Square	df	Sig.
Intercept Only	223.173			
Final	139.618	83.555	16	.000

We can see from Table 6.23 that Perception of Risk (Risk) and Perception of Subjective Norm (SNI) at a 95% confidence level both are significant in explaining the dependent variable for late respondees (observed significances of 0.000 and 0.003 respectively). Perception of Usefulness (Usefulness) and Perception of Ease of Use (Ease) have not proven to be significant (observed significances of 0.208 and 0.979 respectively).

Table 6.23

Likelihood Ratio Tests

Effect	-2 Log Likelihood of Reduced Model	Chi-Square	Df	Sig.
Intercept	143.796	4.179	4	.382
EASE	140.054	.436	4	.979
RISK	164.354	24.736	4	.000
SNI	155.558	15.940	4	.003
USE	145.506	5.888	4	.208

As has been demonstrated above the model was significant for both early and late respondees when tested individually. Both early and late respondees data will now be analysed as a whole for hypotheses testing.

6.10 Hypotheses testing

As an introduction to hypotheses testing, Table 6.24 shows that 65% of the sample either strongly disagreed or disagreed that they would accept the "mark", 13% either strongly agreed or agreed that they would accept the mark.

Table 6.24

Acceptance if it was a major means of transacting

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1.00	69	40.6	48.9	48.9
	2.00	22	12.9	15.6	64.5
	3.00	32	18.8	22.7	87.2
	4.00	16	9.4	11.3	98.6
	5.00	2	1.2	1.4	100.0
	Total	141	82.9	100.0	
Missing	System	29	17.1		
Total		170	100.0		

Table 6.25 shows that the model is very significant (P= 0.000) in explaining the dependent variable, being the acceptance of the "mark" if it was a major means of conducting transactions were via the "mark".

Table 6.25

Model Fitting Information

Model	-2 Log Likelihood	Chi-Square	Df	Sig.
Intercept Only	361.935			
Final	240.693	121.242	16	.000

The 0.335 for McFadden rho (R squared) (refer to Table 6.26) has confirmed that the model has contributed to the explanation of the dependent variable. Systat (1999) p. 569 states that "values between 0.2 and 0.40 are considered very satisfactory".

Table 6.26

Pseudo R-Square

Cox and Snell	.577
Nagelkerke	.625
McFadden	.335

We can see in Table 6.27 that perception of risk (risk), perception of subjective norm (SNI) and perception of usefulness (usefulness) are all significant in explaining the dependent variable at the 95% confidence level for all responses, with P value of 0.000, 0.000 and 0.002. The perception of ease of use (ease) has not proved to be significant with a 0.769.

Table 6.27

Likelihood Ratio Tests

Effect	-2 Log Likelihood of Reduced Model	Chi-Square	Df	Sig.
Intercept	245.868	5.175	4	.270
EASE	242.511	1.818	4	.769
RISK	261.703	21.010	4	.000
SNI	274.070	33.377	4	.000
USE	257.271	16.578	4	.002

6.10.1 Response timing consideration

In consideration of the differences between all of the responses, late and early responses, it was seen that the perceived ease of use variables differences were not significant at the 0.01 level for any of the response groupings. The perception of usefulness was significant for all responses, early responses and for late responders at the 0.01 level with the exception of the perception of usefulness of "not having cards" and for "having medical information" for late responders. The difference here was not seen as fundamental for the credibility of the research given the main theme of the research is a monetary system based on the "mark" rather than the convenience factors of the two elements where there were differences.

From the information above it can be seen that the perceived risk variable was significant for all responses and for late responders but not for early responses at the 0.01 level. The Perception of Subjective Norm variable was significant at the 0.01 level for each group of responders. Overall the differences were not seen to have affected the credibility of the research and the full data will be used to consider the hypotheses used.

6.10.2 Hypotheses testing

In testing the Hypotheses:

H1 Perceived usefulness of a verification mark does not have a direct positive effect on an accountant's attitude towards accepting a verification mark.

The hypothesis is rejected (p= 0.002). Perceived usefulness was seen as important in the acceptance decision, supporting its inclusion into the technology acceptance model from Davis' technology acceptance model (1989).

H2 Perceived risks of a verification mark does not have an inverse effect on an accountant's attitude towards accepting a verification mark.

The hypothesis is rejected (p= 0.000). Perceived risk was seen as important in the acceptance decision (supporting the contribution to the model developed by the author).

H3 The perception that a verification mark would be easy to use would not have a direct positive effect on an accountant's attitude towards accepting a verification mark.

The hypothesis is supported (p= 0.769). Perceived ease of use was not seen as important in the acceptance decision supporting the null hypothesis. This result questions the contributions of the Davis' (1989) acceptance model. Consideration is made as to whether the permanent and personal nature of the verification mark

would detract from the ease of use contribution's importance. In a circumstance of a more perfunctory nature the risk factor would be expected to be lower whilst the ease of use factor would be expected to take on significance. It is considered that the ease of use factor should be retained in the model until these theories have been tested.

H4 The perception of a subjective norm will not have a direct positive effect on an accountant's attitude towards accepting a verification mark.

The hypothesis is rejected (p= 0.000). Perceived subjective norm was seen as important in the acceptance decision which rejects the null hypothesis (0.000). This shows the subjective norms' importance in the acceptance decision and supports the contribution to the model by the author to re-establish it from the Theory of Reasoned Action (Fishbein 1975).

6.11 Classification

Table 6.28 illustrated the model prediction (refer to section 4.7) as compared to the actual observation of the survey. The measures of 1 to 5 represented the likert scale degree from strongly disagree to strongly agree. As shown in the Table, the model successfully predicted 63 strongly disagree decisions out of 69 decisions, which is about 91% of the responses. It did not predict the "strongly agree to accept" responses. The model correctly predicted 50% of the "agree to accept" responses and 69% of the uncertain responses. Overall, the model successfully predicted 66% of the acceptance decisions.

Table 6.28

Classification

Observed	Predicted					
	1.00	2.00	3.00	4.00	5.00	Percent Correct
1.00	63	2	4	0	0	91.3%
2.00	11	0	11	0	0	0.0%
3.00	8	0	22	2	0	68.8%
4.00	1	0	7	8	0	50.0%
5.00	0	0	1	1	0	0.0%
Overall Percentage	58.9%	1.4%	31.9%	7.8%	.0%	66.0%

6.12 Technology Acceptance Model

The responses from the survey were also used to analyse the Technology Acceptance Model developed by Davis (1989). Two independent variables of perceived usefulness and perceived ease of use were used along with the same dependent variable being the

acceptance of the "mark" if it was a major means of conducting transactions were via the "mark". Table 6.29 shows that the technology acceptance model had a significance of 0.327 in explaining the dependent variable (being the acceptance of the "mark" if it was a major means of conducting transactions via the "mark"). This is compared with the modified Technology Acceptance Model (0.000) giving validation to the contributions of the modified Technology Acceptance Model.

Table 6.29

Model Fitting Information

Model	-2 Log Likelihood	Chi-Square	Df	Sig.
Intercept Only	266.389			
Final	139.986	126.404	120	.327

The .349 for McFadden rho (R squared) has confirmed that the model has contributed to the explanation of the dependent variable.

Table 6.30

Pseudo R-Square

Cox and Snell	.592
Nagelkerke	.641
McFadden	.349

Table 6.31

Likelihood Ratio Tests

Effect	-2 Log Likelihood of Reduced Model	Chi-Square	Df	Sig.
Intercept	139.986(a)	.000	0	.
EASE	911.922(b)	771.936	60	.000
USE	216.806(c)	76.820	60	.071

According to the above tables, we can see that Perception of Ease of Use (Ease) is significant in explaining the dependent variable at the 95% confidence level for all responses (P= 0.000). The Perception of Usefulness (Use) has not proven to be significant (p= 0.071).

6.13 Subjective norm – open questions

In an open question relating to the subjective norm, the respondents were asked to "identify four people or groups that you hold as important in your life in terms of the influence their opinions have on you". This question sought respondents' views of the important influences in their opinion forming process. Each respondent was asked to list the people that influenced them in the relevant decisions in descending order of importance. A list of the identified influences and their frequency of being listed, regardless of ranking, is provided below. Appendix 2.1 shows the influences cited as the most important influence, Appendix 2.2 shows the influences cited as the second most important influence, Appendix 2.3 shows the influences cited as the third most important influence, Appendix 2.4 shows the influences cited as the fourth most important influence. It should be noted that the professional bodies failed to be ranked

as the most important source, by any respondent, and only on two occasions were seen as the second most important source and on one occasion the fourth most important influence. In total, only 1% of professional accountants referred to the professional body as an influencing factor.

Table 6.32 All influences cited

Influence	**Number of Citations**	**Influence**	**Number of Citations**
Spouse	62	Clients	2
Children	37	Mentors	2
Friends	36	Discussion groups	1
Family	28	Artists	1
Parents	27	Government	1
Religious institution	20	World	1
Colleagues	18	Academics	1
Community	10	Extended Family	1
Work	7	Elders	1
Self	5	Industry Organisation	1
Community organisation	4	Parents-in-law	1
Professional Body	3	Community heads	1
Sibling	3	Financial	1
Peers	3		

Employer	2	Moral Standards	1
Clients	2	Public figures	1
Mentors	2	Legal	1

To confirm the impression from Table 6.32 the subjective norm was used as the dependent variable and each of the potential influences was used as an explanatory variable (ranking from zero for not represented to one when it was mentioned as the fourth most important influence through to four when it was mentioned as the most important influence). The regression R-squared was 0.403. The professional bodies variable was not significant in determining the subjective norm dependent variable ($t = -1.024$, $p = 0.311$). The only significant contribution, at the 95% confidence level, was that of "clients" ($t = 2.088$, $p = 0.043$). The next most important covariates, significant at the 10% level, were religion ($t = -1.979$, $p = 0.054$), public figures ($t = 1.685$, $p = 0.099$) and friends ($t = -1.710$, $p = 0.094$).

6.14 Perceived ease of use – open questions

The descriptive results in the ease of use section showed a weighting towards respondents perceiving that the various parts of using the system was easy. There were fewer respondents that perceived that the system was difficult or very difficult. The results of the open question highlighted that there was some uncertainty about the difficulty of using the system or how the system would handle various difficulties or overloads.

In an open question relating to factors making the "mark" difficult to use, the respondents were asked to “identify in order of importance up to four factors that they thought might make a “mark” difficult to use”. This question sought their unprompted view of the ease of using the “mark”. Each respondent was asked to list the factors in order of difficulty and these responses were grouped. Technology issues were the most cited (89), attitudinal rejection was next with 51 citations, authority issues was next (32), followed by misuse issues (31), privacy issues (25), health issues (17), human issues (14), security issues (10) and, finally, cost issues (7). Tables containing the details of the responses have been listed in Appendices 3.1 to 3.9.

To confirm the impression from the above information, a regression model was estimated with ease of use as the dependent variable and each of the ease labels as explanatory variables (ranking from zero for not represented to one when it was mentioned as the fourth easiest through to four when it was mentioned as the easiest). The regression R-squared was 0.143. There were only two significant contributions for usefulness, at the 95% confidence level. The label “privacy” ($t = -2.837$, $p = 0.005$) indicating that the larger the concern respondents had about privacy the less easy they determined the “mark” to be. The inference here is that they see the “mark” as adversely affecting the ease of their life as it would make their life less private. The other significant variable was the label “technology” ($t = 2.272$, $p = 0.025$) indicating that significant numbers of respondents felt that the “technology” made the process easier.

6.14.1 Technology issues

The eighty-nine technology issues accounted for 32% of the "difficulty" concerns of the respondents. Of those who responded on technology issues, 52% listed the issue as the most important and 33% listed it as the second most important. A general distrust of the technology was expressed along with distrust of various parts of the technology, specifically, the reader, programming, equipment and "mark". There was also a distrust of the technology under conditions such as high volume, remote locations, various weather conditions or wear and tear. The fact that the technology was to be imbedded was also cause for concern. For instance there was a concern that there may be "changes due to bodily functions". Respondents were also concerned with how changes of personal details would be handled and how various roles of a person and entities would be dealt with. Another major issue raised was concern over the duplication of the "mark". How the system is maintained and verified was also raised in this difficulty section.

6.14.2 Attitudinal rejection issues

The fifty-one attitudinal rejection issues accounted for 18% of the concerns of the respondents. Of those who responded on the attitudinal rejection issue, 71% listed the issue as the most important. Many respondents expressed the view that they or the community simply would not accept this style of technology without offering a reason. Others offered ethical concerns such as violations of "the human body", independence, freedom, dignity, age concerns and other "civil rights" issues.

6.14.3 Authority issues

The thirty-two authority issues accounted for 11% of the concerns of the respondents. Respondents contemplated contributions to the source of their concerns were "authorities", "government" and "big brother". Their concerns included "abuse", "suspicion", "loss of individuality", "control", "fear of unauthorised unofficial monitoring" and "integrity".

6.14.4 Misuse issues

The thirty-one misuse issues accounted for 11% of the concerns of the respondents. Respondents contemplated fraud, misuse and corruption in the system from various perspectives including the accumulation phase, for instance, duplication of the mark, electronic transfer of funds, misuse of the system from a monetary perspective and information misuse including "information theft" and resultant control issues. "Kidnapping" was also mentioned.

6.14.5 Privacy issues

The twenty-five privacy issues accounted for 9% of the concerns of the respondents. Respondents contemplated the "invasion of privacy" from "privacy restrictions", "issues of confidentiality" to "fear of embarrassment- you are over the limit".

6.14.6 Health issues

The seventeen health issues accounted for 6% of the concerns of the respondents. Respondents contemplated a whole range of health concerns from the process including "fear of disease or illness due to implants", the invasiveness of the procedure, "illness factors", allergies, "increased violence re increased information availability' right up to "death".

6.14.7 Human issues

The fourteen human issues accounted for 5% of the concerns of the respondents. Examples of the issues contemplated were "incompetence", "human error" and "duress in use of mark".

6.14.8 Security issues

The ten security issues accounted for 4% of the concerns of the respondents. Respondents contemplated a range of "concerns about security", including the "ability to remove or tamper with marks".

6.14.9 Cost issues

The seven cost issues accounted for 3% of the concerns of the respondents. Respondents contemplated the "cost of implementation". The qualitative comments (refer to Appendix 3.9) include: cost of scanning, cost of implementation, cost of equipment for business, expensive hardware, business acceptance (eg rollout times and cost), administration, and cost.

6.15 Perceived usefulness – open questions

In an open question relating to factors making the "mark" useful, the respondents were asked to "identify up to four issues in order of importance that they thought would make the verification mark useful in a private context". This question sought their unprompted view on the usefulness of using the "mark". Medical issues were the most cited (30), identity issues were next with 26 citations, security issues next (19), followed by recording issues (16), access issues (14) ease issues (12), problems (8), privacy issues (7), protest issues (6), fraud issues (5) and taxation issues (4). Tables containing the details of the responses have been listed in Appendices 4.1 to 4.11.

To confirm the impression of the above information, a regression with usefulness used as the dependent variable, and, each of the uses used as explanatory variables was estimated. Ranking from zero for not represented to one when it was mentioned as the fourth most important use, through to four when it was mentioned as the most important use. The regression R-squared was 0.205. There were only two significant contributions

for usefulness, at the 95% confidence level. The label “privacy” (t = -2.850, p = 0.005) indicating that the larger the concern respondents had about privacy the less useful they determined the “mark” to be. The inference here is that they see the “mark” as adversely affecting their privacy. The other significant variable was the label “easy” (t = 2.250, p = 0.026) indicating that significant numbers of respondents felt that the “mark” made the purchasing process easier which was considered useful.

6.15.1 Medical issues

Medical issues accounted for 20% of the respondents’ perceived usefulness of having a “mark”. Respondents noted that “personal information” such as “medical records” would be “readily available”. Respondents suggested this would be helpful if a person suffered “dementia” or for various “medical emergencies”. One respondent noted that “one would want to be safe in releasing one’s medical information”.

6.15.2 Identity issues

Identity issues accounted for 18% of the respondents’ perceived usefulness of having a “mark”. Respondents suggested the type of information that should be included in the identification such as “name, date of birth, gender, address, age, DNA”, “nationality”, “medical and other”. The use of the identification was at the “airport”, “locating a missing person”, “emergency identification”, “banks, legal circumstances” and “policing identification”.

6.15.3 Security issues

Security issues accounted for 13% of the respondents' perceived usefulness of having a "mark". The following is a representation of respondents' suggestions of the "marks" security usefulness: "preventing" a "terrorist's attack", "illegal access to your records", "individual personal security", "financial information" and the risk of card/data loss". One contributed that the "mark" would be useful at entertainment venues such as "at sports or theatre" implying that knowing the identity of people at entertainment venues would reduce the security threat.

6.15.4 Recording issues

Recording issues accounted for 11% of the respondents' perceived usefulness of having a "mark". Of those who responded on security issues 71% listed the issue as most important. The following is a representation of respondents' suggestions of the "marks" recording usefulness; "planning", "managing financial" information and "consolidation of personal information".

6.15.5 Access issues

Access issues accounted for 10% of the respondents' perceived usefulness of having a "mark". The following is a representation of respondents' suggestions of the "marks" access usefulness. Respondents described an "ability to access" the "mark" as useful and noted that they would "always have the information with them". They mentioned there

would be “no necessity to carry credit cards” and access would be available in a “remote location”.

6.15.6 Ease issues

Ease issues accounted for 8% of the respondents’ perceived usefulness of having a “mark”. There were 12 responses. The “ease of use” was mentioned including the “ease of performance of everyday functions”, the fact that “banking transactions could be easier”, that “paying bills/shopping would be easier” and that there would be “no need for cash or cards”. The characteristics of the “mark” were also seen to be useful including its speed, size and weight.

6.15.7 Problems

In response to the respondents’ perceived usefulness of having a “mark”, 5% of the contributions were problems of the system. The following is a representation of items mentioned, the “mark could be copied”, the “mark could be stolen”, the mark would “still require proof ID”. One respondent wrote “scanners do not yet have a good record of accuracy, I don’t think it would as it would still be subject to major computer flaws so could produce dangerously wrong information. In my 11 years in practice I have seen several examples of bank errors. The fact is the banks do not reconcile their transactions so giving more power to their unreliable data is madness”.

6.15.8 Privacy issues

Privacy issues accounted for 5% of the respondents' perceived usefulness of having a "mark". "Invasion of privacy" and "confidentiality" were a representation of feedback provided.

6.15.9 Protest issues

Some respondents used the perceived usefulness of having a "mark" question to protest about the mark. For instance "I am completely against the use of anything of this nature", "all bad", "none- better solution without the risks are available" and "unable to comment because I morally object to a "Mark". Protest issues accounted for 4% of the references on perceived usefulness of having a "mark".

6.15.10 Fraud issues

Fraud issues accounted for 3% of the respondents' perceived usefulness of having a "mark". "Fraud" and "less chance of fraud" were representative of the contributions.

6.15.11 Taxation issues

Taxation issues such as "control of tax receipts and payment" and "record keeping for tax purposes" accounted for 3% of the respondents' perceived usefulness of having a "mark".

6.16 Perceived risk (control) – open questions

In an open question relating to factors making the "mark" risky to use, the respondents were asked to “List in descending order up to four of your highest concerns relating to risks that a "mark" may bring”**.** This question sought their unprompted view of how risky using the “mark” would be. Each respondent was asked to list the factors in order of how risky using the “mark” would be and these responses were grouped from the largest groups to the smallest groups, regardless of ranking. Privacy issues were the most cited (87), control issues was next with 66 citations, misuse issues was next (42), followed by marketing issues (9), rights issues (7), physical safety issues (5) and finally management issues (4). Tables containing the details of the responses have been listed in Appendices 5.1 to 5.7.

To confirm the impression of the above information a regression model was undertaken, control was used as the dependent variable and each of the classified control risks were used as explanatory variables (ranking from zero for not represented to one when it was mentioned as the fourth most risky control issue, through to four when it was mentioned as the most important control risk) in a regression model. The regression R-squared was 0.054 with none of the contributions being significant.

6.16.1 Privacy issues

Privacy issues accounted for 40% of the respondents' "concerns relating to control over your life that a "mark" may bring. Of those who responded on privacy in their contribution on control risk, 75% listed the issue as most important, 18% listed it as second most important and 7% listed as third most important. The following is a representation of respondents' suggestions of the "marks" control, privacy issues; "invasion of privacy", "secrecy" and "confidentiality". More specifically concerns included the fact that "people can be traced when not necessary" or "watching". "Access to information" was also a concern; for instance, "information on Mark becoming publicly available", "sale of personal details to various organisations", "hasslement by hackers", "invasion of personal information by government & other bodies". It was also commented that there was "insufficient privacy legislation".

6.16.2 Control issues

Control issues accounted for 30% of the respondents' "concerns relating to control over your life that a "mark" may bring", of those who responded on control issues with 69% listing the issue as most important, 27% listed it as second most important and 4% listed it as third most important. The following comments represent respondents' concerns such as a "lack of freedom" relating to the "marks" control issues. Respondents were concerned that the mark would result in authorities, "controlling my life", and more specifically "government control", "big brother watching real time judgments" the

“financial organisations may control my life” and the control “other private organisations have over my life”.

6.16.3 Misuse issues

Misuse issues accounted for 19% of the respondents’ “concerns relating to control over your life that a "mark" may bring”. Those who responded on misuse in their contribution on control were spread with respect to the importance of the issue with 53% listing the issue as highly important, 39% listing it as second most important and 8% listing as third most important. The following is a representation of respondents’ suggestions of the “marks” control, misuse issues. Respondents mentioned “monitoring by undesirable persons”, “misuse of information by government and corporate sectors” and a concern that “any reader can download more data than authorised”. Other concerns included a “lack of security”, “misuse of information”, “fraud”, “identity theft” and “money theft”.

6.16.4 Marketing issues

Marketing issues accounted for 4% of the respondents’ “concerns relating to control over your life that a "mark" may bring”. The following is a representation of respondents’ suggestions of the “marks” control, marketing issues. Respondents noted a “potential for marketers to "suffocate society with their products” with “marketing/ advertising targeted at me”.

6.16.5 Rights issues

Rights issues accounted for 3% of the respondents' "concerns relating to control over your life that a "mark" may bring". The following is a representation of respondents' suggestions of the "marks" control, rights issues. Respondents said that people "should be able to have the right to refuse the mark", "biblical prophecy", that the mark was "too invasive" and generally that it is "all bad".

6.16.6 Physical safety issues

Physical safety issues accounted for 2% of the respondents' "concerns relating to control over your life that a "mark" may bring". The following is a representation of respondents' suggestions of the "marks" control, physical safety issues. Respondents stated an "invasion of your body", "safety (robbery of limb/mark)" and "fear of disease/illness due to implants".

6.16.7 Management issues

Management issues accounted for 2% of the 'respondents' "concerns relating to control over your life that a "mark" may bring". The following is a representation of respondents' suggestions of the "marks" control, management issues. Respondents represented "need for updating of information regularly" others were concerned that it would be "probably too costly to administer" others noted that it would "require imputing of codes or authorisation for parties to use the "mark"".

6.17 Perceived risks (other) – open questions

In an open question relating to risks, the respondents were asked to “identify up to four other risks that you would associate with a "mark". This question sought their unprompted view of the risks of using the “mark”. The responses (142) were grouped from the largest groups to the smallest groups, regardless of ranking. Misuse issues were the most cited (32), control issues was next with 30 citations, health issues was next (28), followed by technology issues (24), privacy issues (22) and finally identity issues (6). Tables containing the details of the responses have been listed in Appendices 6.1 to 6.6.

To confirm the impression of the above information, risk was used as the dependent variable and each of the classified risks was used as an explanatory variable (ranking from zero for not represented to one when it was mentioned as the fourth risky, through to four when it was mentioned as the most risky) in a regression model. The regression R-squared was 0.042 with none of the contributions being significant.

6.17.1 Misuse issues

Misuse issues accounted for 23% of the respondents’ “other risks” associated with the "mark"”. Of those who responded on the misuse issue, 70% listed the issue as the most important. The following is a representation of comments; “fraud”, “blackmail”, “theft”, “abuse”, “black market and manipulation”. “Breach of security” was also noted as a

concern with comments such as “too easy for people to access information” and “private co's using info”. Various forms of discrimination were cited including “racial”, “political” and “financial”.

6.17.2 Control issues

Control issues accounted for 21% of the respondents’ “other risks” associated with a "mark". Of those who responded on the control issue, 82% listed the issue as the most important. The representations were that it would “place ultimate power in some hands” or it would result in “government control”, “control of personal activities” and “control of personal beliefs, attitudes, etc”. Respondents were concerned with a “loss of individual freedom and anonymity”, one noted it was “one step closer to de-humanisation”, another that “a person's history would be too easily available and potentially deny a person benefit of changed ways”. One respondent mentioned it would “create classes of people- outcast” and another that “I'm not ready to become a robot yet”. Other strong reactions were that “a mark would screw up my life” and that “I would refuse to have one. What are you going to do with people like me?”

6.17.3 Health issues

“Health” issues accounted for 20% of the respondents’ “other risks” associated with the "mark". The following is a representation of claims; “external interference with body function by electronic means”, “changes by biological/physiological actions”, “fear of disease/illness due to implants” and “damage through accidents/injury”. Other

contributions included that “a thief can amputate the mark and force you to give them your password” or “physical abuse and theft of "Mark" and transfer to thief”. On that theme, respondents included “kidnapping and or possible extortion”, “personal safety in public” that a person may “steal the person not the card”, that it may result in “self-mutilation if people seek to rid themselves of the mark” right up to “people killing to obtain record via the mark”.

6.17.4 Technology issues

Technology issues accounted for 17% of the respondents’ “other risks” associated with a "mark". Respondents expressed concern about an “over reliance on technology”, one stated “I would have real concern at the possibility of mass data corruption”, another was concerned about “system failure - loss of control of use of mark” and still another was concerned about “accidental damage - vehicle or sport accident”. Respondents were concerned about how to handle a “change of technology” and the need for a “future upgrade of equipment in body” with a “need for replacement/detection of malfunction”. Respondents mentioned that “software is vulnerable to attack” noting that “it’s possible that the mark would be attacked by the virus” and that it would be possible to “lose track on when individual transactions take place (i.e., walking past a scanner)”.

6.17.5 Privacy issues

“Privacy issues” or what one respondent referred to as “surveillance issues” accounted for 15% of the respondents’ “other risks” associated with a "mark". Those who responded on privacy in their contribution on risk were spread with respect to the

importance of the issue with 26% listing the issue as highly important, 48% listing it as second most important and 26% listing as third most important. Respondents were concerned about “accessibility” or a “(perceived) lack of control on information”. One respondent was concerned about “information being accumulated and accessed by 3rd parties”. Examples of third party concerns given by the respondents included, “government”, “private co's”, “family or friends”. One respondent noted that “a person's history would be too easily available and potentially deny person benefit of changed ways- human element of judging by the way a person is today may be ignored - history would rule supreme”. Another said that it would be an “unnecessary intrusion into a persons life” whilst another stated that the result would be the “tracking of less-than-honest / moral transaction such as a brothel visit, strip club etc” which “would be tagged”.

6.17.6 Identity issues

Identity issues accounted for 4% of the respondents’ “other risks” associated with a "mark". Concerns were expressed about an “identity change” perhaps due to a “physical assault for removal and takeover of identity” or by “getting someone else’s mark by mistake”.

6.18 Factors affecting acceptance – open questions

An open question asked respondents about the issues “that would make you accept or reject the "mark"?”. The responses (208) were grouped from the largest group to the

smallest group, regardless of ranking. Control issues were the most cited (53), privacy issues was next with 46 citations, technology issues was next (21), followed by misuse (20), health issues (13), belief issues (10), just no (9), securities issues (8), humanity issues (6), logic issues (5), convenience issues (5), uniqueness issues (4), benefits issues (3), equity issues (2), spouse issues (2) and finally an existence issue (1). Tables containing the details of the responses have been listed in Appendices 7.1 to 7.16.

To confirm the impression from the above information, "acceptance if it was compulsory" was used as the dependent variable and each of the acceptance labels were used as explanatory variables (ranking from zero for not represented to one when it was mentioned as the fourth importance reason for acceptance through to four when it was mentioned as the most importance reason for acceptance) in a regression model. The regression R-squared was 0.161. There were three significant contributions for acceptance, at the 95% confidence level. The label "health" was the most significant ($t = -2.505$, $p = 0.014$) indicating that the chip was seen as adversely affecting a recipient's health. "Security" ($t = 2.361$, $p = 0.020$) indicates that respondents felt that security was important in the acceptance decision. The last significant covariate was the label "just no" ($t = -1.942$, $p = 0.054$) indicating that some respondents would reject the "mark" outright because of its nature.

6.18.1 Control issues

Control issues accounted for 26% of the respondents contributions as to what would make them accept or reject the "mark". Those who responded on control issues were spread with respect to the importance of the issue with 55% listing the issue as most

important, 36% listing it as second most important and 9% listing it as third most important. The following are a representation of respondent's contributions. One respondent contributed that "beauty, strength" and "joy come from uniqueness not control and conformity", another that it was "morally unacceptable to be able to monitor people", still another felt that "I am losing my freedom". One respondent felt that "personal views" "might be databased for someone to form an opinion on my personal traits views and perhaps habits". The government was another common issue here with a concern of "overregulation by government" and a warning to "never trust governments". One respondent went as far as stating that "when society sinks to the level of bureaucratic power I would rather be dead than accept the mark". Big brother was another term used with one respondent contributing that the "big brother syndrome is already too invasive in our lives". The "lack of consent" was another theme with, for example, the contribution that "choice is compromised" and the issue of whether the mark is "voluntary or compulsory" or the "ability to terminate". Other issues included the "marks accessibility", and a concern regarding "unforseen uses".

6.18.2 Privacy issues

"Privacy issues" or "confidentiality" issues accounted for 22% of the respondents' contributions as to what would make them accept or reject the "mark". Of those who responded on privacy, 71% listed the issue as highly important, 22% listed it as second most important and 7% listed it as third most important. The following are a representation of respondent's contributions. One respondent contributed that "humans require privacy of their lives and a choice of what they discuss to whom", some referred to the issue as an "invasion of privacy". One respondent contributed "privacy!!! Why

should the government/business know everything I do?" One response was to "reject-complete history possible". From the last contribution it is understood that the respondee is concerned that the "mark" would trace all financial transactions which would create a full financial history which would not be acceptable in the mind of the respondee.

6.18.3 Technology issues

Technology issues accounted for 10% of the issues stated as to what would make them accept or reject the "mark". The following are a representation of respondents' contributions. One respondent contributed that there was an "inherent distrust of such technology". "Reliability" was an issue at many of the stages of the process from "failure of technology creating "duplication of people's record" to "system failure", to "problems associated with getting your self "logged" on", to "computer hackers and viruses" right up to "update capacity". Some simply felt it was "impossible" or that "it would not work!!!!!!"

6.18.4 Misuse issues

Misuse issues accounted for 10% of the views expressed as to what would make them accept or reject the "mark". "Fraud", "integrity of users", "issues of abuse" and "abuses by third parties" were raised. Trust was an issue with a "lack of trust in private industry" with warnings to "never trust big business" or "banks". One respondent commented and observed that there was a "lack of business ethics" with risks of "incorrect use of data by both government and corporate entities" with "continued

intrusion in form of mass marketing and government data". It was also noted that "legislation has not stopped video and cd fraud" inferring that fraud resulting from the mark could also not be stopped.

6.18.5 Health issues

"Health" issues or "health concerns" accounted for 6% of the items mentioned as to what would make them accept or reject the "mark". Various elements of health were a concern including "health concerns", "life long implant considerations" and even a concern that there is "no guarantee killer drug not implanted to be triggered if certain age reached medical condition diagnosed or wrong political party chosen".

6.18.6 Belief issues

"Belief" issues accounted for 5% of the feedback provided as to what would make them accept or reject the "mark". Respondents felt the mark was "immoral" with one respondent questioning the validity of the research asking "has the ethics chairperson approved of making the questionnaire?". Respondents noted that it is a "complete reversal of all laws of human nature" another noted it is "against my beliefs". "Religious beliefs" were noted with "religious convictions (:the Beast syndrome)" and a reference to the New Testament

> "Then I saw another beast… it causes all, both small and great both rich and poor both free and slave, to be marked on the right hand or the forehead, so that no one can buy or sell unless he has the mark, that is the name of the beast or the number of its name. This calls for wisdom: let him who has understanding reckon the number of the beast,

for it is human number, its number is 666" (Holy Bible, New International Version, Revelation 13:11, 16:13.

6.18.7 Just no

Statements that the mark would not be accepted without other support accounted for 4% of the comments as to what would make them accept or reject the "mark". The following are a representation of respondents' contributions. "Just no thank you", "I would never accept it only an arsehole would" and "none would make me accept the mark", one respondent contributed "death or the mark ------I choose death".

6.18.8 Security issues

"Security" issues accounted for 4% of the items stated as to what would make them accept or reject the "mark". The following are a representation of respondents' contributions. One respondent stated that there were "advantages over other methods of transacting, e.g., "security", another was concerned about the "security of downloaded information" and another about the "personal security of finances".

6.18.9 Humanity issues

Humanity issues accounted for 3% of the claims as to what would make them accept or reject the "mark". The following are a representation of respondents' contributions. One respondent expressed that "we have gone far enough without further degrading

humanity", another that "society/humanity not advanced enough yet" and still another that "we are too anxious to revolutionise age old customs unnecessarily".

6.18.10 Logic issues

"Logic" issues accounted for 2% of the respondents' contributions as to what would make them accept or reject the "mark". The following are a representation of respondents' feedback. One respondent stated that the "burden of use outweighs any perceived benefit" and another that "such test without wholesale adoption and implementation it will not be readily accepted".

6.18.11 Convenience issues

Convenience issues accounted for 2% of the issues stated as to what would make them accept or reject the "mark". The following are a representation of respondents' viewpoints. One respondent contributed that there were "advantages over other methods of transacting" and another contributed that "we should be bar-coded (or marked) at birth to get rid of TFN, ABN, medicare card" with "health insurance cards, AMEX, Diners M/Card B/Card etc…etc…" as another contribution. One respondent simply noted the "ease of use".

6.18.12 Uniqueness issues

“Uniqueness” issues accounted for 2% of the views expressed as to what would make them accept or reject the "mark". The following are a representation of respondents’ comments. One respondent said that the mark “destroys one's uniqueness as a human being”, with another feeling there would be a “loss of individuality” whilst another felt there would be a “loss of individual freedom and anonymity”. One respondent contributed “accept - ID benefits”.

6.18.13 Benefits issues

Benefit issues accounted for 1% of the items mentioned as to what would make them accept or reject the "mark". The following are a representation of respondents’ contributions. One respondent contributed “accept- general usage business” another “wide acceptance- would only use it if it could be used instead of other c/cards”.

6.18.14 Equity issues

Equity issues accounted for 1% of the feedback provided as to what would make them accept or reject the "mark". The respondents’ contributions included “more equitable tax system (accept)” and “more equitable welfare system (accept)”.

6.18.15 Spouse issues

Spouse issues accounted for 1% of the comments as to what would make them accept or reject the "mark". Respondent's contributions included "spouse views/influence" and "spouse would hate the idea!".

6.18.16 Existence issues

One respondent (0.5% of items) referring to the "mark" contributed that "this is putting our very existence in jeopardy". Whilst it is not clear what in particular the respondee is referring to it could be theorised that the "mark" could create a fatal health issue.

Chapter Seven: Conclusion

7.1 Introduction

This research has extended investigation into a completely cashless monetary system making use of implantable chip technology, global positioning satellites and large computer systems. As the monetary system described in this research is original it had not been previously examined in totality. Therefore the literature review was extensive in order to consider each element of the system. The literature revealed that there has been a trend towards an increased use of cashless mediums of exchange along with more sophisticated methods of identifications. The research traced the rapid advancement of the technology required in the system. Evidence was provided that the system described could be currently implemented. The cashless medium of exchange connected with methods of identification have brought with them associated benefits and risks. It was deemed appropriate to research the possible cashless monetary system with personal implantation especially given the significance of the impacts it may have on individuals, the community and the accounting profession.

Literature has revealed that accountants, both from a traditional and critical perspective would be concerned about the effects of the technology discussed on the collection and manipulation of data and the effect it would have on the extension of information both financial and other. Professional accountants were surveyed regarding their views on a cashless monetary system revolving around the use of implantable chip technology and their responses were noteworthy. The group surveyed were representative of

experienced professional accountants. This group are respected for their knowledge in financial and strategic matters and are seen as influential on the public about such matters. Data was not collected for other industry groups or the community in general and therefore the findings are not representative of their opinions. Although the views of the accountants are not representative of the publics views they do serve as an indicator especially as the public may take into consideration the views of accountants as they may be seen as informed in this area. It could be argued that accountants, being more financially literate are more advanced in their understanding of the workings of the described monetary system as their vocation requires an understanding of the financial areas involved and an understanding of technology. It may be that the general public on such matters might be more conservative but could be induced with an education campaign to move towards the more informed accountants' position.

7.2 Acceptance level

Literature revealed the potential use that could be made of the implantable chip technology incorporated as part of a monetary system to solve many of the problems society and governments are facing including national security, identity fraud and money laundering. The fact that 12.7% of respondents either strongly agreed or agreed that they would accept the mark is evidence the system has support even though the majority surveyed did not support the system. Whilst the results of the research do not represent the community's views the results are instructive about their views. The research identified a concern about the risks of the monetary system including risks of

social control, privacy and abuse. Long-term health effects are also of concern to accountants and perhaps the community.

Surprisingly the acceptance level of the monetary system using the implantable chip was lower (9% strongly agreed or agreed) if the technology was to be compulsorily implemented. Perhaps this is a reaction in a democratic society to being enforced to adopt a new system despite the merits it may have.

This research compliments the interest displayed by the Australian government in implantable identity devices as part of the solution to identity fraud and the challenges to national security. Elements of the system described are under current consideration for adoption including the implantable chip by the Australian Law Reform Commission. This research gives an insight into issues that may impact the community in the near future. The results have significance as they have important practical implications for the community.

7.3 Findings

In researching acceptance, the Modified Technology Acceptance Model has contributed to the literature as demonstrated by the fact that the model was significant (0.000) in explaining the dependent variable, being the acceptance of the “mark” if a major means of conducting transactions were via the “mark”. The model had contributed to the explanation of the dependent variable, confirmed by McFadden rho (R squared) of

0.335. The Technology Acceptance Model developed by Davis (1989), on the other hand, had a significance of 0.327.

The research focused on four hypotheses, dealing with the perception of ease of use of the verification mark (H1), the perceived usefulness of the verification mark (H2), the perceived risks of using the verification mark (H3), subjective norm influence on the decision to adopt a verification mark (H4), and their individual effects on an accountant's attitude towards accepting a verification mark. Perception of risk, subjective norm and perception of usefulness were all proved to be significant in explaining the dependent variable at the 95% confidence level for all responses, with 0.000, 0.000 and 0.002, respectively. The perception of ease of use was not proved to be significant ($p = 0.769$). The findings have important implications for the development and modification of acceptance models in general and specifically for technology acceptance models.

7.4 Response bias

The differences between late and early responses was examined and it was seen that the perceived ease of use variables differences were not significant at the 0.01 level for any of the response groupings. It was found that with respect to the perception of usefulness at the 0.01 level, two elements were not significant, those being "not having cards" and "having medical information". The difference here was not seen as fundamental for the credibility of the research given the main theme of the research is a monetary system based on the "mark" rather than the convenience factors of the two elements where there

were differences. The perceived risk variable was not significant for early responders. The Perception of Subjective Norm variable was significant at the 0.01 level for each group of responders. Overall, the credibility of the research were not seen to be affected by the differences and the full data will be used to consider the hypotheses used.

7.5 Open questions

When the contributions established in open questions as the independent variables were used to regress subjective norm as the dependent variable, the only significant contribution, at the 95% confidence level was "clients" ($t = 2.088$, $p = 0.043$). Religion ($t = -1.979$, $p = 0.054$), public figures ($t = 1.685$, $p = 0.099$) and friends ($t = -1.710$, $p = 0.094$) were significant at the 10% level. The professional bodies variable was insignificant in determining the subjective norm dependent variable ($t = -1.024$, $p = 0.311$). It is unsatisfactory that only three professional accountants from the survey would turn to the professional bodies for this level of guidance. The professional bodies should perhaps be more open in their attitude to developing issues addressing this situation.

With a R-squared of 0.054, the dependent variable of perceived risk and the eleven independent variables had no significant contributions, compared to the dependent variable of perceived ease of use and its nine dependent labels with a R-squared of 0.143. There were only two significant contributions for ease of use, at the 95% confidence level being "privacy" ($t = -2.837$, $p = 0.005$) and "technology" ($t = 2.272$, $p = 0.025$). With a R-squared of 0.205, the dependent variable of perceived usefulness and

the eleven dependent variables had two significant contributions for usefulness, at the 95% confidence level being “privacy” (t = -2.850, p = 0.005) and “easy” (t = 2.250, p = 0.026).

7.6 Research Contributions

National security is currently a governmental research priority and the Australian government has recently allocated significant levels of funding in the latest federal budget to promote the interface between research, technology and national security (Australian National Security 2007). This research is of vital interest to the Australian government as it grapples with such matters. The Australian Law Reform Commission (ALRC) has raised the issue of implantable chips or RFID as an identity device in ALRC Issues Paper 31: Review of Privacy. The Commission is following up the issues by soliciting responses from its members about the use of implantable chips as an identity device. Professor Margaret Jackson of RMIT University, School of Accounting and Law, a member of ALRC, solicited the author’s advice via email on the 26 March 2007 on the area and used the response as part of her submission on the issue. This research provides timely information and contributes to the discussion currently occurring and aimed at reforming Australian law.

The system would provide complete and continual real time records for individuals, businesses and regulators and the research showed it was evident that both traditional accounting researchers and critical theorists have reason to consider the diffusion of this verification technology. Benefits and hazards should be weighed from a social perspective including its impact on privacy, possibility of abuse or system corruption

and social control which intrigued Foucault who likened it to Bentham's concept of a Panopticon (Rabinow 1982). Terrorist attacks have made many regulators and communities extremely vigilant culminating in security elevation. Many in the community have voiced their preparedness to forego personal rights for the ability to trace criminals to enhance safety. Perhaps enforcing visitors to Australia to accept an implanted chip may be seen as a necessary security measure. In a community with democratic rights held so strongly the security net may need to be consequentially widened to satisfy the needs of equity. Eventually the measures may embrace residents as well. Such moves are an enormous social threat.

7.7 Recommendations

This research has demonstrated that technology has advanced sufficiently to enable a completely cashless monetary system. It is recommended that a continual research focus be applied to this area to allow a continuing understanding of the systems that are developing and the effects they would have on individuals, society and the profession. There is room in this discipline for a diverse study of the issues including traditional accounting research and critical perspectives. Various accounting disciplines could benefit from ongoing research and could analyse the affects the system would have on continuous reporting, auditing and management systems.

It is recommended that the modified Technology Acceptance Model be used for a broad range of technology acceptance research given the usefulness of the model for this research supported by the statistical analysis.

The modified Technology Acceptance Model shows that influences are important in the acceptance decision and yet only three professional accountants from the survey turned to the professional bodies, which is not significant to the subjective norm influence. It is recommended that the professional bodies embrace this style of emerging research so that members gain confidence in turning to them for direction in emerging areas. It is recommended that the professional bodies embrace a role as a leader in emerging financial issues.

7.8 Further research

Karahanna et al 1999, p. 184 state "from a conceptual standpoint, few empirical studies have made a distinction between individual's pre adoption and post adoption beliefs and attitudes." This current research examined the pre adoption decision in isolation from any adoption decision providing the opportunity to compare this research with adoption and post adoption behaviour and a comparison of results if the system or a similar system is adopted in the future.

In the survey instrument, the word "mark" was used (rather than chip or another acronym). This might have raised negative connotations and associations (including religious) associated with the term. Perhaps acceptance would have been greater had different terminology been used. It is suggested the survey instrument could used again on a similar audience with an alternative term that may raises less negative feelings.

While this research considers professional accountants as one of the major groups having essential influence over the views of society, other professional groups such as computer or information technology experts and lawyers may hold similar influence. Further research could seek the views of other groups and the public as a whole to extend the applicability of the findings.

Bibliography

'A hot, fast chip' 2004, *Straits times*, Singapore, 15 September, p. 26.

'American's allow the implanting of a medical chip in the body for the first time' 2004, *Ming*, Hong Kong, 15 October, p. 30.

'Beer with microchip' 2005, *Herald Sun*, Melbourne, 19 January, p. 7.

'Chipping in for pets' 2004, *Herald Sun*, Melbourne, 5 July, p. 32.

'ETA account rules' 2000, *The Disclosure*, vol. 17, no. 1, pp. 4-7.

'Govt rules out national ID card scheme' 2005, *The Age*. 12 July, p. 15.

'ID card not dealt' 2005, *Herald Sun*, Melbourne, 13th July, p. 15.

'*India: BPO's do it again, Aussie data on sale'* 2005, viewed 6 February 2005, <http://www.asiamedia.ucla.edu/article.asp?parentid=28294>.

'Southern Thais eager for "smart cards"' 2004, *Straits Times*, Singapore, 14 October, p. 42.

'The Privacy Act: your privacy, your choice' 2002, *Herald Sun*, 4 August, pp. 4-5.

'U.S. orders chips for passports' 2004, *International Herald Tribune*, New York, p. 18.

'Warriors ponder appeal to get points back' 2006, *ABC News Online*, 28 February, viewed 29 February 2006, <http://www.abc.net.au/news/newsitems/200602/s1579995.htm>.

'Xerox workers strike over spying' 2004, *The Age*, Melbourne, September 22, viewed 25 September 2004, <http://www.theage.com.au/articles/2004/09/22/1095651385674.html?from=storylhs>.

'*Detecting and Managing A Break-in'* 2003, The International Bank for Reconstruction and Development/The World Bank, viewed 21 December 2006, <http://www.infodev-security.net/handbook/part5-chapter9.shtml>.

Aardsma, T. 2001, 'Smart cards', *Inside the Internet*, vol. 8, no. 3, pp. 3-15.

ABA's Code of Banking Practice: Preamble 1993, Australian Bankers' Association 2004, viewed 12 Jan 2006, <http://www.bankers.asn.au/Default.aspx?ArticleID=95>.

Adams, D., Nelson, R.R. and Todd, P. 1992, 'Perceived usefulness, ease of use, and usage of information technology: A replication', *MIS Quarterly*, vol. 16, no. 2, pp. 227-248.

Agarwal, R. & Prasad, J. 1997, 'The role of innovation characteristics and perceived voluntariness in the acceptance of information technologies', *Decision Sciences*, vol. 28, no. 3, pp. 557-582.

Agre, P.E. & Rotenberg, M. (eds) 1997, *Technology and Privacy: The New Landscape*, The MIT Press, Cambridge.

Aiken, M. 2004, *Macro and Microevolutionary Perceptions of Quality for Accounting Measures and Financial Reporting*, RMIT.

Ajzen, I. & Fishbein, M. 1980, *Understanding Attitudes and Predicting Social Behaviour*, Prentice Hall, Englewood Cliffs NJ.

Ajzen, I. 1991, 'The theory of planned behavior', *Organizational Behavior and Human Decision Processes*, vol. 50, pp. 179-211.

Albrecht, K. & McIntyre, L. 2005, *Spychips: How Major Corporations and Government Plan to Track Your Every Move with RFID*, Nelson Current.

Al-Hajri, S.2005, *Internet Technology Adoption in The Banking Industry*, Victoria University of Technology.

Answers.com 2007, Multinomial logit, viewed 10 July 2007, <http://www.answers.com/multinomial%20logit%20>.
'*Applied Digital Solutions Introduces Verichip'* 2002, viewed 17 December 2002, <http://www.lot49.com/2001/12/applied_digital_solutions_intr.html>
Arnold, B. 2005, *Caslon Analytics Identity Crime*, viewed 12 Jan, <http://www.caslon.com.au/idtheftprofile.htm>.
Assael, H. & Keon, J. 1982, 'Nonsampling vs Sampling error in survey research', *Journal of Marketing*, vol. 46, no. 2, pp. 114-123.
Attorney-General Philip Ruddock 2005, Australian Smart Cards Summit, Sydney Convention Exhibition Centre, 29 June, viewed 3 Nov 2006, <http://www.ag.gov.au/agd/WWW/MinisterRuddockHome.nsf/Page/Speeches_2005_Speeches_29_June_2005_-_Speech_-_Opening_Keynote_Address_to_Australian_Smart_Cards_Summit_2005>
Austen, I. 2004, '"Spoofproof" fingerprint scanners?' *International Herald Tribune*. New York, p. 18, 15 October.
Australian Law Reform Commission (ALRC) 2006, *Review of Privacy*, Issues Paper 31, Commonwealth of Australia, 20 September.
Australian Law Reform Commission 2007, 'Unique Multi-Purpose Identifiers', in *Submission to the Australian Law Reform Commission's Review of Privacy – Issues*, paper 31, 8 March.
Australian Lifestyle Survey 2002, Australia Post, July.
Australian Mutual Provident Society 2002, 'Shareholder news', AMP Shareholder News, February, viewed 30 Nov, <http://www.amp.com.au/group/3column/0,,CH887_SI3,00.html>.
Ax, C. & Bjornenak, T. 2005, 'Bundling and diffusion of management accounting innovations - the case of the balanced scorecard in Sweden', *Management Accounting Research*, vol. 16, pp. 1-20.
Bagozzi, R.P., Davis, F.D., & Warshaw, P.R. 1992, 'Development and test of a theory of technological learning and usage', *Human Relations*, vol. 45, no. 7, pp. 660-686.
Baker, C.R. 2002, 'Crime, fraud and deceit on the internet: is there hyperreality in cyberspace?', *Critical Perspectives on Accounting*, vol. 13, no. 1, pp. 1-16.
Barclay, L. 2004, 'FDA Approves Implantable Chip Used to Access Medical Records', viewed 14 Nov, <http://www.medscape.com/viewarticle/491994>.
Barki, H. & Hartwick, J. 1994, 'Measuring user participation, user involvement, and user attitude', *MIS Quarterly*, vol. 18, no. 1, pp. 59 – 82, March.
Bayley, D. 2004, *Fractional Biometrics: A solution to Privacy and Anonymity in Fingerprint Identification*, RMIT University - School of Business Computing - Research Series, Melbourne.
Benbasat, I. 1985, 'An analysis of research methodologies', in MacFarlan, W. (eds), *The Information Systems Research Challenge, Proceedings of Harvard business School colloquium*, HBS Press, Boston, MA, pp. 47-85.
Bentham, J. 1791, *Panopticon, or the Inspection-House*, Tate, Edinburgh, vol. 4, pp. 37-171.
Black, A. 2003, 'Coins in a slot on the way out', *Herald Sun*, Melbourne, p. 21.
Blaikie, A. & Utz, C. 2000, *The Ralph Report*, Sydney, June 6, viewed 20 Nov 2005, <http://www.claytonutz.com/downloads/project06.pdf>
Bollen, R. 2001, 'The regulation of internet banking', *Journal of Banking and Finance Law and Practice*, vol. 12, pp. 5-17.

Bowers, D.G. 1976, *Systems of Organisation: Management of the Human Resource*, University of Michigan Press.
Brancheau, J.C. & Wetherbe, J.C. 1990, 'The adoption of spreadsheet technology: Testing and extending innovation diffusion theory in the context of end user computing', *Information Systems Research*, vol. 1, no. 2, pp. 115-143.
Brancheau, J.C. 1987, *The Diffusion of Information Technology: Testing and Extending Innovation Diffusion Theory in the Context of End User Computing*, Unpublished doctoral dissertation University of Minnesota.
Broadbent, J. 1995, 'The values of accounting and education: Some implications of the Creation of visibilities in schools', *Advances in Public Interest Accounting*, vol. 6, pp. 69-98.
Bunney 2003, 'Security benefits', *Fraud intelligence*, vol. 1, pp. 10-13, December/January.
Burtstin, F. 2002, 'Licence tampering fear - holograms over photos', *The Herald Sun*, 12 June, p. 1.
Cale, E.J.J. & Eriksen, S.E. 1994, 'Factors affecting the implementation outcome of a mainframe software package: A longitudinal approach', *Information and Management*, vol. 26, pp. 165-175.
Callon, M. 1991, 'Techno-economic networks and irreversibility', in Law, J. (ed.), *A Sociology of Monsters: Essays on Power, Technology and Domination*, Routledge, London and New York, pp. 132-161.
Carroll, B. 2002, 'Price of privacy: Selling consumer databases in bankruptcy', *Journal of Interactive Marketing*, vol. 16, no. 3, pp. 47-58.
Chaudhuri, A. 1998, 'Product class effects on perceived risk: The role of emotion', *International Journal of Research in Marketing*, vol. 15, no. 2, pp. 157-168.
Chin, W.W. & Gopal, A. 1995, 'Adoption intention in GSS: Relative importance of beliefs', *Data Base Advances*, vol. 26, no. 2 & 3, pp. 42-64.
Chongruksut, W. 2002, *The Adoption of Activity-Based Costing in Thailand*, Victoria University.
Christensen, G.E. 1987, *Successful Implementation of Decision Support Systems: An empirical Investigation of Usage Intentions and Behaviour,* Unpublished doctoral dissertation, University of California.
Clarke, R. 1994, 'Human identification in information systems: Management challenges and public policy issues', *Information Technology & People*, vol. 7, no. 4, pp. 6-37.
Colombo, R. 2000, 'A model for diagnosing and reducing nonresponse bias', *Journal of Advertising Research*, vol. 40, no. 1 & 2, pp. 85-93.
Company: Corporate FAQ 2006, VeriChip Corporation, viewed 25 February 2007, <http://www.verichipcorp.com/content/company/corporatefaq#r7>.
Compeau, D. & Higgins, C. 1995, 'Application of social cognitive theory to training for computer skills', *Information System Research*, vol. 6, no. 2, pp. 118-143.
Connors, E. & Moullakis, J. 2005, 'High-tech blitz on bank fraud', *Financial Review*, Melbourne, 16 September, p. 1 & 68.
Considine, B., Razeed, A., Lee, M. & Collier, P. 2005, *Accounting Information Systems: Understanding Business Processes,* John Wiley & Sons Australia, Qld.
Conway, D. 2005, 'PM plays terror card', *The Age*, 18 July.
Cooper, R.B. & Zmud, R.W. 1990, 'Information technology implementation research: A technological diffusion approach', *Management Science*, vol. 36, no. 2, pp. 123-139.

Courtis, J.K. 1982, 'Private shareholders response to corporate annual reports', *Accounting and Finance*, pp. 53-72.
Courtis, J.K. 1989, 'Perception data-gathering: A note on mail questionnaire methodology and bias', *Pacific Accounting Review*, vol. 2, no. 1, pp. 118-135.
Covacio, S. 2003, 'Technological problems associated with subcutaneous microchips for human identification', *Informing Science + IT Education Conference*, Pori, Finland.
Crain, W.C. 1985, *Theories of Development*, Prentice-Hall.
Crawford, C. 2005, 'Bank email fraud alert', *Herald Sun*, 19 June, p. 31.
Crawford, C. 2005, 'Wanted: Home for sex-crazed maniac: New laws to allow spying on Mr Baldy', *Herald Sun*, 10 April, p. 11.
Creswell, J.W. 1994, *Research Design: Qualitative and Quantitative Approaches*, Sage, London.
Crews, C.W. 2002, *Human bar Code: Monitoring Biometric Technologies in a Free Society*, Cato Policy Analysis, no. 452, Cato Institute.
Crowley, M. 1999, *Smart Cards: Some Social Implications*, Monash University School of Business and Electronic Commerce Working Paper Series, Monash Uni School of Business & Electronic Commerce, Churchill Victoria, pp. 1 – 33.
CyberSource, Electronic Check Processing, viewed 29 February 2007, <http://www.cybersource.com/products_and_services/electronic_payments/electronic_check_processing/>.
Davis, F.D. & Venkatesh, V. 1996, 'A critical assessment of potential measurement biases in the technology acceptance model: Three experiments', *International Journal of Human-Computer Studies*, vol. 45, no. 1, pp. 19-45.
Davis, F.D. 1989, 'Perceived usefulness, perceived ease of use and user acceptance of information technology', *MIS Quarterly*, vol. 13, no. 3, pp. 319-340.
Davis, F.D. 1993, 'User Acceptance of Information Technology: System Characteristics, User Perceptions, and Behavioral Impacts', *International Journal of Man Machine Studies*, vol. 38, no. 3, pp. 475-487.
Davis, F.D., Bagozzi, R.P. & Warshaw, P.R. 1989, 'User acceptance of computer technology: A comparison of two theoretical models', *Management Science*, vol. 35, no. 8, pp. 982-1004.
De Lange, P.A. 2000, *A Model of Student Progress for Business Undergraduates Studying via Open Learning*, Monash University.
De Souza, R.J. 1997, *Silicon Micromachined Tactile Imagers for use in Live-Scan Fingerprinting and Credit Card Applications*, Engineering, Michigan.
De Vaus, D.A. 2002, *Surveys in Social Research*, 5th edn, Allen & Unwin, NSW.
Dean, R. 2004, 'A right to privacy', *Australian Law Journal*, vol. 78, pp. 114-125.
DeLone, W.H. & McLean, E. 1992, 'Information system success: The quest for the dependent variable', *Information Systems Research*, vol. 3, no. 1, pp. 60-95.
Diamond, S.S. 2000, Reference Guide on Survey Research, 2nd edn, in *Reference Manual on Scientific Evidence*, Washington, DC: The Federal Judicial Center, pp. 229-276.
Dorries, B. 2006, 'You little rippers', *Herald Sun*, Melbourne, 15 October, p. 15.
Dowsley, A. 2006, 'Mr Baldy locked up', *Herald Sun*, Melbourne, 16 August, p. 1-2.
Doyle, C. & Bagaric, M. 2003, 'The right to privacy and corporations', *Australian Business Law Review*, vol. 31, no. 4, pp. 237-250.
Dreyfus, H.L. & Rabinow, P. 1982, *Michel Foucault: Beyond Structuralism and Hermeneutics*, Harvester Press Brighton, England.

Dubois, F. 2001, 'Oburther on the future of smart cards', *Electronic Commerce News*, Potomac, vol. 6, no. 2, pp. 1-5.
Eatons, J. 1999, '"Open Sesame?" - the problems of digital identity and secure access to information in the Internet era: issues for the information industry', *EBusiness Information Review*, vol. 16, no. 4, pp. 184-191.
Edwards, R. 2004, 'Electronic payments and the pull back', *Insolvency Law Journal*, vol. 12, no. 2, pp. 81-94.
ElAmin, A. 2006, RFID advances help food traceability, *Decision News Media SAS*, 1 Dec, viewed 12 January 2007, < http://www.foodproductiondaily-usa.com/news /ng.asp?n=65062-idtechex-rfid-traceability>.
Ellison, C. 2006, Revised exposure draft of anti-money laundering and counter-terrorist financing Bill released for public comment, July 13, viewed 3 Nov, <http://www.ag.gov.au/agd/WWW/justiceministerHome.nsf/Page/Media_Releases _2006_3rd_Quarter_13_July_2006_-_Revised_exposure_draft_of_anti-money__ laundering_and_counterterrorist_financing_Bill__released_for_public_comment>.
Engberg, S.J., Harning, M.B. & Jensen, C.D. 2004, *Zero-knowledge Device Authentication: Privacy & Security Enhanced RFID preserving Business Value and Consumer Convenience*, Second Annual Conference on Privacy, Security and Trust, New Brunswick, Canada, IMM Publications.
eSign, 'Gatekeeper & ABN Digital Certificates', esign Australia Limited, 2001.
eSign, 'PKI Delivery Methodology overview', esign Australia Limited, 2001.
eSign, 'Securing your business', esign Australia Limited, 2001.
Everett-Green, R. 1996, *Britannica book of the Year (1996): 'Computers and Information Systems, Special Report, Cyberspace*', Encylopaedia Britannica Inc, Chicago.
Exploration of Future Electronic Payments Markets 2006, Department of Communications, Information Technology and the Arts, Commonwealth of Australia, June.
FAQ # 959 2005, SAS Institute Inc, viewed 10 July 2007, <http://support.sas.com/faq/ 009/FAQ00959.html>.
Feder, B. & Zellar, T. 2004, 'A gain for chips in people', *International Herald Tribune*, New York, 15 October, p. 18.
Feder, B.J. & Zeller, T. Jr 2004, 'Identity Chip Planted Under Skin Approved for Use in Health Care', *The New York Times*, New York, 14 Oct, pp. 1-4.
Federal Government launches National Animal Identification System 2006, RFid Gazette, 6 February, viewed 10 March 2007, <http://www.rfidgazette.org/2006/02/ federal_governm.html>.
Federal Privacy Commissioner 2004, *Community Attitudes Towards Privacy*, Sydney, p. 104.
Feige, E.L. 2000, *Taxation for the 21st Century: The Automated Payment Transaction (APT) Tax*, Forthcoming in Economic Policy, University of Wisconsin-Madison, October.
Ferguson, C.B. 1995, *The Differential Effects of Human Computer Interfaces on Accountants using Microcomputers*, Accounting and Finance, Melbourne University, Melbourne.
Ferguson, C.B. 1997, 'The effects of microcomputers on the work of professional accountants', *Accounting and Finance*, vol. 37, no. 1, pp. 41-47.
Ferguson, J. 2005, 'Smartcard's dumb side', *Herald Sun*, Melbourne, 10 August, p. 18.

Festervand, T.A., Snyder, D.R. & Tsalikis, J.D. 1986, 'Influence of catalog versus store shopping and prior satisfaction on perceived risk', *Journal of the Academy of Marketing Science*, vol. 14, no. 4, pp. 28-36.
Field, A. 2000, 'Electronic commerce, encouragement from Canberra', *Law Institute Journal*, vol. 74, no. 5, pp. 54-57.
Fielding, N.G. & Fielding, J.L. 1987, *Linking Data*, Beverly Hills, CA: Sage.
Financial Stability Report, Reserve Bank of New Zealand 2005, viewed 14 December 2006, <http://www.rbnz.govt.nz/finstab/fsreport/fsr_may2005.pdf>.
Firewall 2007, SearchSecurity.com Definitions, viewed 21 December 2006, <http://searchsecurity.techtarget.com/sDefinition/0,290660,sid14_gci212125,00.html>.
Fishbein, M. & Ajzen, I. 1975, *Belief, Attitude, Intention and Behaviour: An Introduction to Theory and Research*, Addison-Wesley.
Fleischman, R.K. & Tyson, T.N. 2000, 'The interface of race and accounting: the case of the Hawaiian sugar plantations 1835-1920', *Accounting History*, May, pp. 7-32
Fong, T. 2006, 'Cellphone thefts fall for first time in three years', *The Straits Times*, Singapore, 25 July, p. 1.
Forbes, C. 2004, 'This cutting room flawed', *Herald Sun*, Melbourne, 14 November, p. 9.
Forzley, M. 2006, 'E-Commerce banks on alternative payment boom', *E-Commerce Times*, 25 October, viewed 23 November 2006, <http://www.technewsworld.com/story/53866.html>.
Foucault, M. 1975, *Discipline and Punish*, Gallimard (France), France.
Foucault, M. 1982, *Discipline and Punish*, Peregrine Books, Middlesex.
France-Presse, A. 2006, 'A mobile network that keeps track of everything you do', *Strait Times,* Singapore, p. 9.
Francis, J. 1990, 'After Virtue? Accounting as a moral and discursive practice', *Accounting, Auditing and Accountability Journal*, vol. 3, no. 3, pp. 5-17.
Fraud The Facts 2006, APACS, viewed 4 December 2006, <http://www.apacs.org.uk/resources_publications/documents/FraudtheFacts2006.pdf>.
Frenkel, J. 2005, 'Cash for patients' records', *Herald Sun*, Melbourne, 25 May, p. 1 & 4.
Friedman, R.I. 2000, *Red Mafiya: How the Russian Mob Has Invaded America*, Brown, Boston.
Funnell, W. 1998, 'Accounting in the service of the holocaust', *Critical perspectives on Accounting*, vol. 9, no. 4, pp. 435-464.
Funnell, W. 2001, 'Accounting for justice', *Accounting Historians Journal*, vol. 28, no. 2, pp. 187-206.
Gee, J. 2003, 'Criminal identity crisis', *Australian CPA*, vol. 73, no. 8, pp. 66-68.
Gibbs, N. 2002, 'Apocalypse now', *Time*, 1 July, pp. 38-46.
Giles, T. 2004, 'Tighter DNA laws', *Herald Sun*, Melbourne, 23 November, p. 14.
Gobel, T.F. & Regan, A.C. 2001, 'Impacts of information technology on personal travel and commercial vehicle operations: research challenges and opportunities', Transportation research, Part C – emerging technologies, vol. 9, p. 87-121, April.
Godschalk, H. and Krueger, M. 2001, *Why E-Money Still Fails*, Card Forum International, Sep/Oct, pp. 24-27.
Goo, S. 2003, 'US proposes big brother security system for airlines', *The Age*, Melbourne, 10 September, p. 1.
Goodwin, D. & Kloot, L. 1996, 'Strategic communication, budgetary role ambiguity, and budgetary response attitude in local government', *Financial Accountability & Management*, vol. 12, no. 3, pp. 191-204.

Gottliebsen, R. 2003, 'Smarter thinking merits rewards', *The Australian*, Melbourne, 10 February, p. 28.
Gowland, D.J. 2000, *The Public Sector Transformation to Privatisation and Cultural Implications*, Faculty of Law and Management, La Trobe University.
Grabosky, P.N. & Smith, R.G. 1997, *Current and Emerging Patterns of Fraud*, Australian Institute of Criminology.
Gray, J.H. & Densten, I.L. 1998, 'Integrating Quantitative and Qualitative Analysis Using Latent and Manifest Variables', *Quantity & Quality*, vol. 32, no. 4, pp. 419-431.
Green, E. 1999, 'We need to think straight about electronic payments', *Journal of Money, Credit, and Banking,* vol. 31, no. 2-3, pp. 668-670.
Greenemeier, L. 2006, Standard key to smart card use, *InformationWeek*, 29 May, viewed 1 December 2006, <http://www.andreae.com/New_releases_of_interest/Selected_press_releases_2006_ May.htm>.
Haberfield, I. 2003, 'Fears of debt trap for young', *Herald Sun*, Melbourne, p. 9.
Haberfield, I. 2004, 'DNA solves 1500 crimes Prisoner sample pay off', *Herald Sun*, Melbourne, p. 21.
Haberfield, I. 2004, 'Licence to gamble', *Herald Sun*, Melbourne, 23 March, p. 5.
Haberfield, I. 2005, 'All your past on card of future', *Herald Sun*, Melbourne, 20 November, p. 22.
Hair, J.F., Anderson R.E, Tatham R.L. & Black W.C 1992, *Multivariate Data Analysis with Readings*, MacMillan Publishing Co. New York.
Halamka, J. 2005, 'Straight from the shoulder', *The New England Journal of Medicine*, vol. 353, no. 4, pp. 331-333.
Hale, J.L., Householder, B.J., & Greene, K.L. 2003, The theory of reasoned action, in J.P. Dillard and M. Pfau (eds.), *The Persuation Handbook: Developments in Theory and Practice,* Thousand Oaks, CA: Sage, pp. 259 - 286.
Halliday v Nevill (1984) 155 CLR 1; 59 ALJR 124
Ham, P. 2002, 'Cleaning up in sumurf land', *CA Charter*, pp. 56-60.
Hansen, J. 2001, 'In the shadow of big brother', *Connect*, 20 January, pp. A22-A23.
Harper, I. Simes, R. & Malam, C. 2005, *The Development of Electronic Retail Payments Systems*, Paper for the International Telecommunications Society Conference, 23 August.
Hartwick, J. & Barki, H. 1994, 'Explaining the role of user participation in information system use', *Management Science*, vol. 40, no. 4, pp. 440-465.
Harvey, M. & Mickelburough, P. 2005, 'ID card back on agenda', *Herald Sun*, Melbourne, 16 July, p. 17.
Haskett, D. & Ziegenfuss, D. 1999, 'Developing a strategy to control credit card fraud', *Cost Management*, vol. 13, no. 7, pp. 16-21.
Hendrickson, A. R., Massey, P. D., & Cronan, T. P. 1993, 'On the test-retest reliability of perceived usefulness and perceived ease of use scales', *MIS Quarterly*, vol. 17, no. 2, pp. 227-230.
Heng, S. 2004, 'E-payments: modern complement to traditional payment systems', *Economics,* Deutsche Bank Research, no. 44, May 6.
Henry, P. 2006, *Office of Access for ID Smart Cards Trials*, Open Interchange Consortuim, Melbourne, p. 1.
Hilberg, R. 1985, *The Destruction of the European Jews*, Holmes and Meir, Holmes and Meir, New York.

Hillhouse, I. 2005, 'Privacy in perspective', *National Accountant*, vol. 21, no. 2, pp. 44-45.
Hines, R. 1988, 'Financial accounting: In communicating reality, we construct reality', *Accounting, Organizations and Society*, vol. 13, no. 3, pp. 251-61.
Ho, S. & Ng, V. 1994, 'Customers' risk perceptions of electronic payment systems', *International Journal of Bank Marketing*, vol. 12, no. 8, p. 14.
Hoffer, J.A. & Alexander, M.B. 1992, The diffusion of database machines', *ACM SIGMIS Database*, ACM Press, vol. 23, no. 2, pp. 13-19.
Holmstrom, J. & Stalder, F. 2001, 'Drifting technologies and multi-purpose networks: the case of the Swedish cashcard', *Information and Organisation*, Elsevier, vol. 11, no. 3, pp. 187-206, July.
Hopper, T. & Armstrong, P. 1999, 'Cost Accounting, Controlling labour and the rise of conglomerates', *Accounting, Organizations and Society*, vol. 16, no. 5-6, pp. 405-438.
Houghton, J.W. & Vickery, G. 2005, *Working Party on the Information Economy*, Organisation for Economic Co-operation and Development, p. 105.
Icke, D. 2001, *Children of the Matrix: How an Interdimensional Race Has Controlled the World for Thousands of Years-and Still Does*, Bridge of love, Wildwood, USA.
Igbraia, M., Zinatelli, N., Cragg, P. & Cavaye, A. 1997, 'Personal computing acceptance factors in small Firms: A structural equation model', *MIS Quarterly*, vol. 21, no.3, pp. 279-305.
Ioannis, A. 2000, *Integration of an Electronic Purse in a GSM Subscriber Identity Module*, Munich University of Technology, viewed 1 December 2006, <http://www.ics.forth.gr/~asko/Master_Thesis_Report.pdf>.
Ives, B., Olson, M.H. & Baroudi, J.J. 1983, *The Measurement of User Information Satisfaction*, ACM Press, New York, USA.
Jackson, M. 2003, 'Internet privacy', *Telecommunications Journal of Australia,* vol. 53, no. 2, pp. 21-31.
Jacoby, J. & Kaplan, L.B. 1972, 'The components of perceived risk', in M. Venkatesan (eds), *Third Annual Conference of the Association for Consumer Research*, Association for Consumer Research, College Park, MD, pp. 382-93
Jakobsson, M. 2007, *The Human Factor of Phishing*, Indiana University, Bloomington, viewed 14 January 2007, < http://www.informatics.indiana.edu/markus/papers/aci.pdf>.
Johnston, B. 1997, 'Underground cash fears', *Information Management & Computer Security*, vol. 5, no. 1, p. 35.
Johnston, R.P. 2005, 'A tour of tomorrow's technology', *Journal of Accountancy*, vol. 200, no. 4, pp. 95-97, October.
Karahanna, E. & Limayem, M. 2000, 'E-mail and V-mail usage: Generalizing across technologies', *Journal of Organizational Computing and Electronic Commerce*, vol. 10, no.1, pp. 49-66.
Karahanna, E., Straub, D.W. & Chervany, N.L. 1999, 'Information technology adoption accross time: A cross-sectional comparison of pre-adoption and post adoption beliefs', *MIS Quarterly*, vol. 23, no. 2, pp. 183-213.
Kasim, S. 2004, 'Full roleout of MyKad', *New Straits Time Press*, Berhad Malaysia, 15 January, p.1.
Kraut, R.E., Dumais, S.T. & Koch, S. 1989, *Computerization, Productivity, and Quality of Work-Life*, ACM Press, New York, USA.

Kreltszheim, D. 2003, 'The legal nature of "electronic money" Part 2', *Journal of Banking and Finance Law and Practice*, vol. 14, pp. 261-287.
Kreltszheim, D. 2003, 'The legal nature of "electronic money": Part 1', *Journal of Banking and Finance Law and Practice*, vol. 14, pp. 161-184.
Krzanowski, W.J. 1998, *An Introduction to Statistical Modelling*, Arnold, London.
Kwon, T.H. & Zmud, R.W. 1987, *Unifying the Fragmented Models of Information Systems Implementation, in Critical Issues in Information Systems Research,* John Wiley and Sons ltd, Chilchester England.
Lane, M. 2003, 'Would a microchip keep your child safe?', *BBC News Online Magazine*, viewed 28 November 2005, <http://news.bbc.co.uk/2/hi/uk_news/magazine/3307471.stm>.
Lapsley, I. and Wright, E. 2004, 'The diffusion of management accounting innovations in the public sector: a research agenda', *Management Accounting Research*, vol. 15, no. 3, pp. 355-374.
Latest body art trend: 'invisible' tattoos 2006, *ABC News*, 6 February, viewed 21 May 2006, <http://abcnews.go.com/Technology/popup?id=2339802>.
Latour, B. 1996, *Aramis or the Love of Technology*, Havard Press.
Lee, M. 2004, 'Share and Swap without wires', *Strait Times*, Singapore, 28.
Lepofsky, R. 2004, 'Preventing Identity Theft', *Risk Management*, vol. 51, no. 10, p. 34.
Lepore, S.J., Kling, R., Iacono, S. & George, J. 1989, Implementing Desktop Computing, Infrastructure, and Quality of Worklife, *International Conference on Information Systems*, Boston, Massachusetts, United States, ACM Press.
Levy, S. 2002, *Crypto: Secrecy and Privacy in the New Code War*, Penguin, London.
Lim, N. 2003, *The Effects of Experience and Perceptions on Consumers' Acceptance of Online Shopping*, The University of Queensland.
Lin, Y. 2005, *Understanding Students' Technology Appropriation and Learning Perceptions in Online Learning Environments*, University of Missouri, Columbia.
Ling, S. 2001, 'DBS goes into debit', *Straits Times*, Singapore, p. 21.
Littleton, A.C. 1953, *Structure of Accounting Theory*, American Accounting Association.
Long, R.J. 1993, 'The impact of new office information technology on job quality of female and male employees', *Human Relations*, vol. 46, no. 8, pp. 939-962.
Lyons, D. 1993, *Moral Aspects of Legal Theory: Essays on Law, Justice and Political Responsibility*, Cambridge University Press.
Macedo, R. 2004, 'Catching their chips', *Herald Sun*, Melbourne, p. 39.
Mancey, I. 2004, '24-Hour Satellite patrol on beasts', *The Sun*, England, p. 34.
Mandela, N. 1955-59, 'Journal of Democratic Discussion', *Liberation*.
Mara, B. 2000, 'The Internet and Financial Services', *Journal of Banking and Financial Services*, vol. 114, no. 5, pp. 6-11.
Markoff, J. 2006, 'Study Say Chips in ID Tags are vulnerable to Viruses', *New York Times*, Technology Section, p. 23.
Mathieson, K. 1991, 'Predicting user intensions: Comparing the technology acceptance model with the theory of planned behavior', *Information Systems Research*, vol. 2, no. 3, pp. 173-191.
Matlack, C., Djemai, K. & Fairlamb, D. 2002, 'A cash-free France? Don't bet the store', *Business week*, November, p. 1-2.
McAndrews, J.J. 1999, 'E-money and payment system risks', *Contemporary Economic Policy*, vol. 17, no. 3, pp. 348-357, July.

McIver, J.P. & Carmines, E.G. 1981, *Unidimensional Scaling*, Beverly Hills, Sage publications.
Mcllveen, L. 2003, 'Hackers steal top secrets', *Herald sun*, 11 November, Melbourne, p. 5.
McLuhan, M. & Powers, B. 1981, 'Electronic Banking and Death of Privacy', *Journal of Communication*, vol. 31, no. 1, pp. 164-169.
McManus, G. 2004, 'ID not on the cards', *Herald Sun*, Melbourne, p. 7.
Medcof, J.W. 1989, 'The effect of extent of use of information technology and job of the user upon task characteristics', *Human Relations*, vol. 42, no. 1, pp. 23-41.
Metlikovec, J. 2003, 'Smart move for tourism', *Herald Sun*, Melbourne, p. 17.
Metrejean, E., Smith, H.G. & Elam, D 2004, *A Call for Accounting Education on Computer Crime and Ethics*, Accounting Information Systems Educator Conference.
Mexican officials get chipped 2004, Wired, 13 July, viewed 20 December 2006, <http://www.wired.com/science/discoveries/news/2004/07/64194>.
Michael, K. & Michael M.G. 2005, 'Microchipping people: The rise of the electrophorus', *Quadrant*, vol. 49, no. 3, pp. 22-33, March.
Michael, K. & Michael, M.G. 2006, 'The Proliferation of Identification Techniques for Citizens throughout the Ages', in K. Michael and M.G. Michael (eds), *The Social Implications of Information Security Measures on Citizens and Business,* University of Wollongong, NSW, pp. 7-26.
Miller, K. 2005, *Communications Theories: Perspectives, Processes, and Contexts*. New York: McGraw-Hill.
Mitchell, M. & Jolley, J. 1988, *Research and Design Explained*, Holt Rinehart Winston, New York.
Moor, K. 2002, 'Call for National ID scheme to foil crime', *Herald Sun*, Melbourne, 11 June, p. 1.
Moor, K. 2002, 'Fraud a threat: Choose your identity from the internet', *Herald Sun*, Melbourne, 12 June, p. 28.
Moore, G.C. & Benbasat, I. 1991, 'Development of an Instrument to Measure the Perceptions of Adopting an Information Technology Innovation', *Information System Research*, vol. 2, no.3, pp. 192-222.
Moore, G.C. & Benbasat, I. 1996, 'Integrating diffusion of innovations and theory of reasoned action models to predict utilization of information technology by end users', in *Diffusion and Adoption of Information Technology*, K. Kautz and J. Pries-Heje (eds.), Chapman and Hall, London, pp. 132-146.
Morfuni, V. 2004, 'Legal professional priviledge and the government's right to access information and documents', *Australian Tax Review*, vol. 33, no. 2, pp. 89-121.
Morgan, F.W. 1990, 'Judicial standards for survey research: an update and guidelines', *Journal of Marketing*, vol. 54, no. 1, pp. 59-70.
Morgan, R. 2001, Privacy and the Community, Federal Privacy Commissioner, July 2001, viewed 21 December 2006, <http://www.privacy.gov.au/publications/rcommunity.html>.
Morrissey, T. 2005, 'Swans tech big step', *Herald Sun*, p. 35.
Moullakis, J. 2005, 'Low score for report card on laundering', *The Australian Financial Review*, Melbourne, 21 October, p. 12.
Moullakis, J. 2005, 'Smartcard tardiness increases risks', *Financial Review*, Melbourne, 16 September, p. 68.

Murray C.J. 2002, 'GPS makes inroads in personal security technology', *Electronic Engineering Times*, 19 August 2002, p. 4.
Murray, C.J. 2002, 'Injectable chip opens door to "human bar code"', *Electronic Engineering Times*, 1 April 2002, viewed 31 January 2003, <www.eetimes.com/story/OEG20020104S0044>.
Neiger, D. 2002, 'Feeling insecure?', Australian CPA, vol. 72, no. 5, pp. 54-55.
Neuman, L. 1997, *Social Research Methods: Qualitative and Quantitative Approaches*, Boston: Allyn and Bacon.
Nicholson., B. 2003, 'Health care trial sparks ID debate', *The Age*, Melbourne, p. 2.
Nilakanta, S. & Scamell, R,W. 1990, 'The effect of information sources and communication channels on the diffusion of innovation in a data base development environment', *Management Science*, vol. 36, no. 1, pp. 24-40, January.
Niman, N. 1985, *The Economics of an Electronic System of Exchange*, Economics, Texas University, Texas, p. 111.
Panko, R.R. 1991, 'Is office productivity stagnant', *MIS Quarterly*, vol. 15, no. 2, pp. 191-204.
Papadakis, M.C.C. 2005, 'DNA kit for kids', *Herald Sun*, Melbourne, 3 April, p. 30.
Pardas, A. 2004, 'Hoping for better apps from MyKad', *New Straits Times*, Berhad Malaysia, 5 January, p. 2.
Parthasarathy, M. & Bhattacherjee, A. 1998, 'Understanding post adoption behaviour in the context of on-line services', *Information Systems Research*, vol. 9, no. 4, pp. 362-379.
Pavri, F.N. 1988, *An Empirical Study of the Factors Contributing to Microcomputers Use*, The University of Western Ontario, Ontario, Canada.
Peet, M. 1999 Spoken language interfaces gaining acceptance as technology matures, The Edge, Vol. 3, no. 4, pp. 1-4.
Pentland, B.T. 1989, *Use and Productivity in Personal Computing: An Empirical Test*, ACM Press, New York, USA.
Phillips, G. 2004, 'Chipping away at our privacy', *Herald Sun*, Melbourne, 21 October, p. 21.
Phillips, S. 2004, 'Footy's future shock', *Herald Sun*, Melbourne, 25 September, p. 21.
Prescott, M.B. & Conger, S.A. 1995, 'Information technology innovations: A classification of IT locus of impact and research approach', *Data Base*, vol. 26, no. 2-3, pp. 20-41.
Pricewaterhousecoopers 2001, 'Risk Management forecast: 2001', Pricewaterhousecoopers.
Privacy, Opportunity International Australia 2006, viewed 21 December 2006, <http://www.opportunity.org.au/home.asp?pageid=1279F63F6C612F99>.
Quinn, J.B., Baruch, J.J. & Paquette, P.C. 1987, 'Technology in services', *Scientific American*, vol. 257, no. 6, pp. 24-32.
Rabinow, P. 1982, *The Foucault Reader*, Penguin Books.
Rafaeli, A. 1986, 'Employee attitudes toward working with computers', *Journal of Occupational Behaviour*, vol.7, pp. 89-106.
Ramesh, E. M. 1997, 'Time Enough? Consequences of Human Microchip Implantation Risk', *Risk*, Franklin Pierce Law Centre, vol. 8, p. 373.
Ranum, M. 2000, 'Intrusion detection maintains an unblinking eye on IS security', *Edpacs,* vol. 27, no. 11, p. 1-5.

Ratnasingam, P. 2001, 'Electronic commerce adoption in Australia and New Zealand', *Malaysian Journal of Computer Science*, vol. 14, no. 1, p. 1-8.
Riley, R. 2003, 'Hi-tech chips to verify identity', *Herald Sun*, Melbourne, 29 June, p. 2.
Riley, T. 1998, 'Me and my electronic shadow: privacy - a rising trend', *Business Information Review*, vol. 15, no. 2, pp. 83-91.
Risk Management For Electronic Banking And Electronic Money Activities 1998, viewed 4 December 2006, <http://www.bis.org/publ/bcbs35.pdf>.
Roberts, E.S. 1999, 'In defence of the survey method: An illustration from a study of user information satisfaction', *Accounting and Finance*, vol. 39, pp. 53-77.
Robey, D. 1979, 'User attitudes and management information system use', *Academy of Management Journal*, vol. 22, no.3, pp. 527-538.
Rogers, E.M. 1976, 'New product adoption and diffusion', *Journal of Consumer Research*, vol. 2, no. 4, pp. 290-301.
Rogers, E.M. 1983, *The Diffusion of Innovations*, 3rd edn, Free press, New York.
Roselius, T. 1971, 'Consumer rankings of risk reduction methods', *Journal of Marketing*, vol. 35, pp. 56-61, November.
Rosenberg, A. 1983, *The Philosophical Implications of the Holocaust*, Barham.
Rotchanakitunmuai, S. 2005, Exploring the Antecedents of electronic Service Acceptance: Evidence from Internet Secutities Trading, *Proceedings of the Fourth International Conference on eBusiness*, November 19-20, Bangkok, Thailand.
Rubinstein, M. 1988, 'Portfolio Insurance and Market Crash', *Financial Analysis Journal*, January-February, pp.38-47.
Ryan, T.P. 1997, *Modern Regression Methods*, Wiley.
Sadowsky, G., James, X.D., Greenberg, A., Barbara, J.M. & Schwartz, A. 2003, *IT Security for Technical Administrators, Information Technology Security Handbook*, The World Bank, viewed 21 December 2006, <http://infodev-security.net/handbook/part5.pdf>.
Saga, V.L. & Zmud, R. 1994, 'The Nature and Determinants of IT Acceptance, Routinization, and Infusion', *Diffusion, Transfer and Implementation of Information Technology*, in L. Levine (ed.), Proceedings of the IFIP TC8 Working Conference, Pittsburgh, pp. 11–13 October 1993, Amsterdam: Elsevier, pp.67–86.
Saitz, G. 2003, 'Under your thumb', *Star Ledger*, International Biometrics Group, January 30, viewed 26 March 2003, <www.biometricgroup.com/in_the_news/star_ledger.html>.
Sapsford, R. 1999, *Survey Research*, London, Sage Publications.
Shannon, J. 2003, *A companion to business statistics*, Pearson, Frenchs Forest, NSW.
Shapiro, C. 2000, 'Will E-Commerce erode liberty?', *Havard Business Review*, May-June, pp. 189-196.
Shaw, M. 2005, 'Privacy laws may be tightened', *The Age*, Melbourne, 16 August, p. 5.
Sickler, M. 2002, A human implanted with microchips Identification cards in the marketing, viewed 21 February 2007, <http://www.michaeljournal.org/chipID.htm>.
Smith, G. 2004, 'These ID tags get under your skin', *Business Week*, McGraw-Hill, 2 August.
Smith, P.G. & Merritt, G.M. 2002, *Proactive Risk Management: Controlling Uncertainty in Product Development*, Productivity Press, USA.
Sneddon, M. 1997, 'Cyberbanking: remote banking using the internet', Australian Business Law Review, vol. 25, pp. 64-67.

Solomon, E. 1991, *Electronic Money Flows the Moulding of a New Financial Order*, Kluwer Academic Publishers, Boston.
Spence, H.E., Engel, J.F. & Blackwell, R.D. 1970, 'Perceived risk in mail-order and retail store buying', *Journal of Marketing Research*, vol. 7, no. 3, pp. 364-369.
Spot, O. 2005, 'Odd Spot', *The Age*, Melbourne, 5 September, p. 3.
Stein, R. 2006, 'Use of implanted patient-data chips stirs debate on medicine vs. privacy', *The Washington Post*, 15 March, p. A01.
Stewart, A. 2006, A shot-in-the-arm microchip could save your life, 7 August, viewed 29 August 2006, <http://www.nj.com/news/ledger/stories/microchip_0807.html>.
Strasser, G. 1998, 'Digital money', *Economics*, Southern California, Southern California, p. 173.
Stuber, G. 1996, *The Electronic Purse: An Overview of Recent Developments and Policy Issues*, Bank of Canada, Canada, January.
Sullivan, L. 2005, 'Georgia court system hopes to trial RFID', *Information Week*, January, viewed 14 November 2006, <http://www.informationweek.com/story/showArticle.jhtml?articleID=57703442>.
Sullivan, L. 2005, RFID System Prevented a Possible Infant Abduction, InformationWeek, 19 July, viewed 28 November 2005, <http://www.informationweek.com/story/showArticle.jhtml?articleID=166400496>.
Summers, G.F. & Hammonds, A.D. 1969, 'Toward a paradigm for respondent bias in survey research', *The Sociological Quarterly*, vol. 10, no. 1, pp. 113-121.
Systat 1996, Systat, 8. Chicago, SPSS.
Systat 1999, Statistics 1. Chicago, SPSS.
Taylor, P. 2002, Public Service Announcement.
Taylor, S. & Todd, P.A. 1995, 'Understanding information technology usage- A test of competing models', *Information Systems Research*, vol. 6, no. 2, pp. 144-176.
The Holy Bible, New International Version, New York International Bible Society 1979.
The Theory of Reasoned Action, Adapted from Understanding Attitudes and Predicting Human Behavior, I. Ajzen and M. Fishbein, 1980. Prentice Hall, Englewood New Jersey, viewed 15 December 2006, <http://www.fw.msu.edu/outreachextension/thetheoryofreasonedaction.htm>.
The world's largest trade exchange - Bartercard guarantees to grow your business, Bartercard. 2006. http://www.bartercard.co.nz/index.asp?pageID=2145829501
Thompson, R. L., Higgins C. A. & Howell J. M. 1994, 'Influence of experience on persona; computer utilization: Testing a conceptual model', *Journal of management Information Systems*, vol. 11 no. 1, pp. 167-187.
Thompson, R. L., Higgins, C., & Howell, J. M. 1991, 'Personal computing: toward a conceptual model of utilization', *MIS Quarterly*, vol. 15 no. 1, pp.125-143.
Tigre, P.B. & Dedrick, J. 2002, Globalization and Electronic Commerce: Environment and Policy in Brazil, Center for Research on Information Technology and Organizations, *Globalization of IT*, paper 307, 1 October.
Timson, L. 2003, 'Phones that make you go mmmm', *The Age*, Melbourne, 9 September, p. 7 & 9.
Tinkler, C. 2006, 'Fake IDs hit clubs', *Herald Sun,* Melbourne, 16 August, p. 2.
Tornatzky, L.G. & Katherine, J.K. 1982, 'Innovation Characteristics and Innovation Adoption-Implementation: A Meta-Analysis of Findings', *IEEE Transactions on Engineering Management*, vol. 29, no. 1, pp. 28-45.

Triandis, H.C. 1980, 'Values, attitudes, and interpersonal behavior', in Howe, H E, (eds), Nebraska Symposium on Motivation, 1979: Beliefs, Attitudes, and Values, University of Nebraska Press, Lincoln, NE, pp. 195-259.
Trojan horse (computing), viewed 10 March 2007, <http://en.wikipedia.org/wiki/Trojan_horse_(computing)>.
Trump, D. 2004, 'I have never used an ATM I rarely use cash', *New Straits Times*. Singapore, 15 September, p. 51.
Tryfos, P. 1996, *Sampling Methods for Applied Research, Text and Cases*, Wiley.
Use This Application Form for Original Registration as an Individual Tax Agent 1936, Australian Government - Australian Tax Office, viewed 30 November 2006, <http://www.tabd.gov.au/forms/downloads/nat525.pdf>.
Van den Poel, D. & Leunis, J. 1999, 'Consumer acceptance of the internet as a channel of distribution', *Journal of Business Research*, vol. 45, no. 3, pp. 249-256.
Van der Stede, W.A., Young, S.M. & Chen, C.X. 2005, 'Assessing the quality of evidence in empirical management accounting research: The case of survey studies', *Accounting, Organizations and Society*, vol. 30, no. 7-8, pp. 655-684.
Van Fossen, A. B. 2003, 'Money Laundering, Global Financial Instability, and Tax Havens in the Pacific Islands', *The Contemporary Pacific*, vol. 15, no 2, pp. 237–275.
Velayutham, S. & Perera, M. 1996, 'The influence of underlying metaphysical notions on our interpretation of accounting', *Accounting, Auditing and Accountability Journal*, vol. 9, no. 4, pp. 65-85.
Venkatesh, V. & Davis, F.D. 1994, 'Modeling the Determinants of Perceived Ease of Use', *Proceedings of the Fifteenth International Conference on Information Systems*, J. I. DeGross, , S.L. Huff, & M.C. Munro (eds.), Vancouver, British Columbia, pp. 213-227.
Wahlert, G. 1996, 'Implications of the Move to a Cashless Society: Law Enforcement' in A. Graycar and P. Grabosky (eds), *Money Laundering in the 21st Century: Risks and Countermeasures*, Canberra, Australian Institute of Criminology.
Wallace, R. 2003, 'Zero Tolerance on welfare fraud', *Herald Sun*, Melbourne, 14 May.
Walsham, G. 1997, 'Actor-network theory and IS research: current status and future prospects', *Proceedings of the IFIP TC8 WG 8.2 international conference on Information systems and qualitative research*, Chapman & Hall.
Wang, Y., Lin, H. & Tang, T. 2003, 'Determinants of user acceptance of internet banking: an empirical study', *International Journal of Service Industry Management*, vol. 14, no. 5, pp. 501-519.
Warren, S. & Brandeis, L. 1890, 'The right to privacy', *Havard Law Review*, vol. 4, pp.193-220.
Wenske, P. 2003, 'Wide web of deceit', *Herald sun*, Queensland, p. 92.
Whittaker, R. 1999, *The End of Privacy: How Total Surveillance is becoming a Reality*, New York Press.
Woodford, M. 1998, 'Doing without money: controlling inflation in a post-monetary world', *Review of Economic Dynamics*, vol. 1, no 1, p. 173-219.
Wright, M. 2002, 'Patterns of purchase loyalty for retail payment method', *International Journal of Bank Marketing*, vol. 20, no. 7, pp. 311-315.
Yong, J.A. 2006, 'Singaporeans on their guard using ATM's', *The Sunday Times*, 1 October, p.1.
Yoshida, J. 2001, Euro Bank Notes to embed RFID chips by 2005, EETimes Online, viewed 14 November, <http://www.eetimes.com/story/OEG20011219S0016>.

Young, A.M. 2003, 'Verification systems the way of the future', National Accountant, vol.19, no. 5, pp. 69-70.
Young, A.M. 2004, 'Acceptance of an implantable date security chip to facilitate a cashless society', *Human Perspectives in the Internet Society: Culture, Psychology and Gender*, K. Morgan, C.A. Brebbia, J. Sanchez, & A. Voiskounsky (eds), WIT Press.
Young, A.M. 2006, 'Privacy issues of using cashless mediums of exchange over the internet', in *The Internet Society II: Advances in Education, Commerce and Government*, K. Morgan, C. A. Brebbia, J. M. Spector (eds), Southampton: WIT Press, pp. 443-447.
Young, P. 2003, 'Sacrifice aids dole rort', *Herald Sun*, Melbourne, 25 May, p. 26.
Zaltman, G., Duncan, R. & Holbeck, J. 1973, *Innovations and Organisation*, John Wiley & Sons.
Zikmund, W. G. 1991, *Business Research Methods*, 3rd edn, HBJ College Publishers, Orlando, Florida.

Appendix 1 Descriptive statistics from closed questions.

1.1 Professional affiliation of respondents

Professional body	% Percent
ICA's	27.0
CPA's	62.4
Both	10.6
Total	100.0

1.2 Gender of respondents

Gender	% Percent
Female	18.4
Male	81.6
Total	100.0

1.3 Age of respondents

Age	% Percent
20-29	5.0
30-39	18.4
40-49	31.2
50-59	35.5
60+	9.9
Total	100.0

1.4 Years in the profession of the respondents

Years in profession	% Percent
0-5	3.5
6-10	13.5
11+	83.0
Total	100.0

1.5 Salary of the respondents

Salary	% Percent
0-$30,000	4.4
$30,000-$60,000	15.4
$60,000-$100,000	38.2
Over $100,000	41.9
Total	100.0

1.6 Position of the respondents

Position	% Percent
Partner	66.4
Manager	5.0
Senior	6.4
Assistant	21.4
Other	.7
Total	100.0

1.7 Field of work of the respondents

Field of work	% Percent
Auditing	18.4
External reporting	1.4
Public sector	7.1
Finance	.7
Information management and technology	1.4
Small business	36.9
Strategic business management	6.4
superannuation	7.1
Taxation insolvency and reconstruction	14.2
Financial planning	.7
Other	5.7
Total	100.0

1.8 Perception of the respondents regarding the ease of the physical registration process

Ease of the physical registration process	% Percent
Very Hard	7.8
Hard	4.3
Neutral	22.7
Easy	36.9
Very Easy	28.4
Total	100.0

1.9 Perception of the respondents regarding the ease of the administration of registering of the "mark"

Easy administration registration	% Percent
Very Hard	6.4
Hard	2.8
Neutral	18.4
Easy	46.1
Very Easy	26.2
Total	100.0

1.10 Perception of the respondents regarding the ease of access to information using the "mark"

Easy access	% Percent
Very Hard	5.0
Hard	4.3
Neutral	21.3
Easy	48.1
Very Easy	21.3
Total	100.0

1.11 Perception of the respondents regarding the ease of using the "mark" to buy and sell

Ease to buy and sell	% Percent
Very Hard	7.8
Hard	8.5
Neutral	29.8
Easy	36.2
Very Easy	17.7
Total	100.0

1.12 Perception of the respondents regarding the ease of using the "mark" for payments over the phone or on the computer

Easy payment over phone or computer	% Percent
Very Hard	5.7
Hard	7.8
Neutral	29.8
Easy	37.6
Very Easy	19.1
Total	100.0

1.13 Perception of the respondents regarding the ease of using the "mark" to create company records

Easy company records	% Percent
Very Hard	9.2
Hard	12.1
Neutral	24.8
Easy	39.7
Very Easy	14.2
Total	100.0

1.14 Perception of the respondents regarding the usefulness of packages using the information created by the "mark"

Useful packages	% Percent
Useless	7.1
Not Useful	15.6
Neutral	27.7
Useful	32.6
Very Useful	17.0
Total	100.0

1.15 Perception of the respondents regarding the usefulness of taxation information created by the "mark"

Useful taxation information	% Percent
Useless	12.1
Not Useful	15.6
Neutral	29.1
Useful	27.7
Very Useful	15.6
Total	100.0

1.16 Perception of the respondents regarding the usefulness of not needing cards because of the "mark"

Useful not having cards	% Percent
Useless	9.9
Not Useful	9.2
Neutral	20.6
Useful	29.8
Very Useful	30.5
Total	100.0

1.17 Perception of the respondents regarding the usefulness of having medical and other information on the "mark"

Useful having medical information	% Percent
Useless	9.2
Not Useful	8.5
Neutral	21.3
Useful	36.9
Very Useful	24.1
Total	100.0

1.18 Perception of the respondents regarding the risk of government social control due to the "mark"

Risk of government social control due to the "mark"	% Percent
Highly decreased	1.4
Decreased	5.0
Neutral	5.7
Increased	22.7
Highly increased	65.2
Total	100.0

1.19 Perception of the respondents regarding the risk of government control via affiliations due to the "mark"

Risk of government social control via affiliations due to the "mark"	% Percent
Highly decreased	1.4
Decreased	5.0
Neutral	8.5
Increased	18.4
Highly increased	66.7
Total	100.0

1.20 Perception of the respondents regarding the risk of bank control due to the "mark"

Risk of bank control	% Percent
Highly decreased	2.1
Decreased	9.2
Neutral	10.7
Increased	24.1
Highly increased	53.9
Total	100.0

1.21 Perception of respondents regarding the risk of private organisation control due to the "mark"

Risk of private organisation control	% Percent
Highly decreased	2.8
Decreased	7.8
Neutral	13.5
Increased	21.3
Highly increased	54.6
Total	100.0

1.22 Perception of the respondents regarding the risk protection regarding the "mark" afforded by legislation

Risk protection from legislation	% Percent
Highly decreased	20.6
Decreased	3.5
Neutral	14.9
Increased	21.3
Highly increased	39.7
Total	100.0

1.23 Perception of the respondents regarding the risk protection provided by constitution regarding the "mark"

Risk protection from the constitution	% Percent
Highly decreased	14.2
Decreased	6.4
Neutral	15.6
Increased	21.3
Highly increased	42.6
Total	100.0

1.24 Perception of the respondents regarding the risk of lost privacy due to companies receiving additional information because of the "mark"

Risk of privacy from companies	% Percent
Highly decreased	2.8
Decreased	7.8
Neutral	12.1
Increased	23.4
Highly increased	53.9
Total	100.0

1.25 Perception of respondents regarding the risk of abuse from companies due to the "mark"

Risk of abuse from companies	% Percent
Highly decreased	3.5
Decreased	5.7
Neutral	7.8
Increased	29.1
Highly increased	53.9
Total	100.0

1.26 Perception of respondents regarding the risk of fraud reduced

Risk of fraud reduced	% Percent
Highly increased	4.3
Increased	17.7
Neutral	19.9
reduced	27.0
Highly reduced	31.2
Total	100.0

1.27 Perception of respondents regarding the risk of theft reduced

Risk of theft reduced	% Percent
Highly increased	7.1
Increased	16.3
Neutral	22.7
reduced	22.7
Highly reduced	31.2
Total	100.0

1.28 Perception of respondents regarding the risks reduced by software encryption

Risks reduced by software encryption	% Percent
Highly increased	1.4
Increased	11.3
Neutral	18.4
Reduced	25.5
Highly reduced	43.3
Total	100.0

1.29 Perception of respondents regarding the risks of temporary corruption

Risks of temporary corruption	% Percent
Very low	5.0
Low	3.5
Neutral	6.4
High	39.7
Very High	45.4
Total	100.0

1.30 Perception of respondents regarding the risks of permanent corruption

Risks of permanent corruption	% Percent
Very low	5.0
Low	5.0
Neutral	24.8
High	25.5
Very High	39.7
Total	100.0

1.31 Perception of respondents regarding the risks of health issues

Risks of health issues	% Percent
Very low	6.4
Low	16.3
Neutral	34.0
High	23.4
Very High	19.9
Total	100.0

1.32 Perception of respondents regarding the risks of offending religious groups

Risks of offending religious groups	% Percent
Very low	12.8
Low	7.1
Neutral	26.2
High	21.3
Very High	32.6
Total	100.0

1.33 Perception of respondents regarding the risks of offending community groups

Risks of offending community groups	% Percent
Very low	17.0
Low	11.3
Neutral	34.0
High	22.0
Very High	15.6
Total	100.0

1.34 Perception of respondents regarding the risks of conflicting with family views

Risks of conflicting with family views	% Percent
Very low	30.5
Low	7.1
Neutral	30.5
High	18.4
Very High	13.5
Total	100.0

1.35 Respondents perceptions regarding whether groups find using the "mark" easy to use

Groups find it easy to use	% Percent
Very Hard	9.2
Hard	16.3
Neutral	32.6
Easy	31.2
Very Easy	10.6
Total	100.0

1.36 Respondents perceptions regarding whether groups find the "mark" useful

Groups find it useful	% Percent
Useless	15.6
Not Useful	18.4
Neutral	38.3
Useful	23.4
Very Useful	4.3
Total	100.0

1.37 Respondents perceptions regarding whether groups find the "mark" risky

Groups find it useful	% Percent
Not risky	48.2
Not Very Risky	24.8
Neutral	18.4
Risky	7.1
Very Risky	1.4
Total	100.0

1.38 Perception of respondents regarding whether the "mark" technology is available

The mark technology is available	% Percent
Not Available	19.1
Not Very Available	21.3
Neutral	26.2
Available	20.6
Very Available	12.8
Not Available	100.0

1.39 Perception of respondents regarding whether the technology surrounding the "mark" is available

The other technology is available	% Percent
Not Available	12.1
Not Very Available	13.5
Neutral	23.4
Available	34.0
Very Available	17.0
Not Available	100.0

1.40 Perception of respondents regarding whether the combined "mark" technology is available

The combined technology is available	% Percent
Not Available	12.1
Not Very Available	22.0
Neutral	29.8
Available	22.0
Very Available	14.2
Not Available	100.0

1.41 Perception of respondents regarding the acceptance of the "mark" by groups

Acceptance by groups	% Percent
Highly Reject	48.2
Reject	29.8
Neutral	17.0
Accept	5.0
Highly Accept	0.0
Total	100.0

1.42 Perception of respondents regarding the acceptance if the "mark" was a major means of transacting

Acceptance if it was a major means of transacting	% Percent
Highly Reject	48.9
Reject	15.6
Neutral	22.7
Accept	11.3
Highly Accept	1.4
Total	100.0

1.43 Perception of respondents regarding the acceptance of the "mark" if it was compulsory

Acceptance if it was compulsory	% Percent
Highly Reject	68.1
Reject	12.1
Neutral	11.3
Accept	6.4
Highly Accept	2.1
Total	100.0

Appendix 2 Influences cited as most important influence

Appendix 2.1 Most important influence (subjective norm – open question)

Influence	Number of citations	Influence	Number of citations
Spouse	43	Community	2
Family	14	Mentors	1
Religious institution	9	Discussion groups	1
Children	5	Artists	1
Self	5	Government	1
Parents	4	Colleagues	1

Appendix 2.2 Influences cited as the second most important influence

Influence	Number of citations	Influence	Number of citations
Children	19	Friends	7
Spouse	13	Religious institution	4
Parents	11	**Professional Body**	2
Colleagues	10	Sibling	1
Family	9	Community	1

Appendix 2.3 Influences cited as the third most important influence

Influence	Number of citations	Influence	Number of citations
Friends	11	Mentors	1
Parents	11	Extended Family	1
Children	8	Parents-in-law	1
Work	7	Mentors	1
Family	5	Clients	1
Spouse	4	Community heads	1
Colleagues	4	Elders	1
Community	3	Industry Organisation	1
Sibling	2	Academics	1
Religious institution	2		

Appendix 2.4 Influences cited as the fourth most important influence

Influence	**Number of citations**	**Influence**	**Number of citations**
Friends	18	Spouse	2
Children	5	Parents	1
Religious institution	5	**Professional Body**	1
Community	4	Public figures	1
Colleagues	3	Legal	1
Peers	3	World	1
Employer	2	Moral Standards	1
Clients	2		

Appendix 3 Perceived ease of use (open question)

Appendix 3.1 Technology issues

Technology issues	Technology issues	Technology issues	Technology issues
Failures of any Technology within process	Inherent distrust of such technology	The Technology could fail	technology down time when Information may not be accessible
Normal Technical Failure	System being down	System Failure	System Failure
Equipment failure	Equipment failure/ Down time would render the mark inoperable for the duration. Credit cards however can be used manually in the event of Computer Scanner Failure.	Machines "down"	Reliability Issues
Faulty	Worry re errors	Trust of the system	Ability to alter
Malfunction of the Mark, Equipment (External)	Damage to "Mark"	Damage, wear (after years of use)	Power failure/ Blackout
Failure of Power	Power failure	Weather Interruptions to Satellites	Weather
Computer Error-Programming impurity/mistakes	Viruses affecting software	Faulty scanner, Other equipment	Computer Error-Scanner Malfunction, Reading in INFO to Using Computer
Possibility of false readings	Malfunctioning requiring access/ replacement of Mark	Access to readers in remote area	Could be deleted by magnetic force
Possibility of false readings	Malfunctioning requiring access/ replacement of Mark	Access to vouching point	Flat batteries in mobiles
technology down time when Information may not be accessible	Technology must be available	Standardisation of Marks & Associated hardware	Data corruption
Subject to tampering	The scanner has an identification specific to each chip	Method of Implanting	Number of Transactions

Where Info changes- Extract Replacement of mark or reprogramming.	Marks- Moving or heating (Chipped Ostriches sometimes move through body)	location of the mark	Differing Thickness of the skin
Changes due to bodily functions	Remote location lack of access to technology	The mark may be unable to be used for International transactions due to the difference of technology capacity for each country	Electronic Devices /Data can be duplicated
Ability to copy the Mark	Potential to copy	Transferring of chip "person to another"	Duplication
One would want to be certain that in releasing information to an appropriate user they could not access other information eg here's my credit card no but I don't want you to know my account balance & you would want to release certain info to your employee (Vice Versa)	Size	Accessibility	Position
Speed	Accuracy	Storage capacity	updating record
changing financial institutions	Maintenance	Maintaining Integrity/Functionality of mark	Future emphasis on updates (Convenience of)
Change of Residence	Change in other personal Details	Death of a personnel & Legal access to the mark	Availability to extract the mark from employees- would this be compulsory on leaving?
Changing employment	Every business needs a reader	Extracting the mark should a personnel be sacked	Retirement Departure
Use of mark Ltd To One Person	One identification insufficient	More than one job	Use by non individuals
Dissecting transactions between various entities controlled by one or more people.	Not Easy to Mark population	Verification	Proof of payment without hard copy
Would it be 100%	Past mistakes are	Comes in eg genetic	Is this a Life time

fail proof in terms of use	imprinted forever	version.	device what happens when the next wave of technology I would not like to be going around saddled with a horse cart?
Comes in eg genetic version. I would not like to be going around saddled with a horse cart.			

Appendix 3.2 Attitudinal rejection issues

Attitudinal rejection	**Attitudinal rejection**	**Attitudinal rejection**	**Attitudinal rejection**
Rejection by majority	Refusal by people	Need for 100% population to carry one	All Factors , I am completely against the use of anything of this nature
Personal opposition to the concept	willingness to be implanted	People acceptance to implant mark	Don't believe we should have implants
Resistance to use	Public dislike	I Like my independence	Civil Rights
Public acceptance	Public acceptance	General Public acceptance	Objection by person
Move over Ned Kelly. I will be joining you	People would not like this	Public Acceptance-Spectrum	Who wants to Agree to having it
Objection to implantation-Physical objection	A permanent invasion	Whether people would allow themselves to be marked	People would trust the integrity of the system
Public Resistance	Acceptance	Individual resistance to implant or Scanner access	Buyers and sellers using cash
Getting the implant into people with their permission	Consent	Objection by Individual to be implanted	the whole concept is objectionable and offensive
Involves dehumanising	Privacy Human Dignity,	Understanding, power, Corruption	Personal freedom(Right to

aspect	Individuality	eg Magnetic	Trade without receiving mark
Anti civil rights	Resistance to such technology (too Invasive)	Objection to implantation- Ethical objection	Market acceptance & ability to Use
Whether people would allow themselves to be marked	Long Education process	Age of consent	Elderly people
Weather the mark can be terminated	Ethical Considerations	The fact that its implanted in your body its a permanent invasion	Depends where its implanted
Violation of the human body	The fact that its implanted in your body its		

Appendix 3.3 Authority issues

Authority issues	Authority issues	Authority issues	Authority issues
Duration of Authority	Geographical Areas of Authority of Aus + cfn2	Authority to issue	Reporting to authorities a nightmare
Changes in Authority level for marked personal	Who would police the authorisation of things	Abuse by government etc	Personal Freedom Big Brother issues
Big Brother	Suspicion about its misuse by authority Big Brother	Control of implanting	There is to much "Control" already
Who Controls the information on the marks	Big Brother is watching and research on this types seems to be a complete waste of public money	Who Controls the information on the marks	Suspicion about its misuse by authority Big Brother
Big Brother Control	Suspicion about its misuse by authority Big Brother	Loss of Individuality and Big Brother Issue	Fear of Big Brother -Being used for Unauthorised Official monitoring
People feel too controlled	Public Perception of Social Control	Fear of unauthorised unofficial monitoring	Integrity of system
People would trust the integrity of the system	Agents could have difficulty	Need to identify who the individual was acting for:-	Purchasing on Behalf of someone else i.e. The Partners of the firm
Company employees :- Change Employment	Maintaining Integrity/Functionality of mark	Potential of unknown transaction	Marks reluctance- who Gets Info

Appendix 3.4 Misuse issues

Misuse issues	Misuse issues	Misuse issues	Misuse issues
May open a whole new range of fraudulent behaviour	Potential Fraud	Fraudulent use of a scanner by 3rd parties	Fear of fraud
The capacity for electronic theft of identity & money is enormous. Who thought up this idea?	Understanding, power, Corruption eg Magnetic	Scanned without authority	Mark being used for purposes not authorised
Potential of misuse	Misuse	Unauthorised interferences occurring	Unauthorised access to information
Computer Fraud	Transacting on another persons behalf	Fraud	Fraud
Counterfeits	Counterfeiting	Fraudulent use (By Replacement of mark)	Concern of Duplication
Forged or transfer Mark	Improper duplication of a Mark	Electronic Devices /Data can be duplicated	Information theft
Unauthorised scanning/Interrogation of work "Auschwitz" tag	Who Controls the information on the marks	People may "Sabotage" the mark	Physically remove or use someone else mark
Cash business	Confidentiality	Kidnapping	

Appendix 3.5 Privacy issues

Privacy issues	**Privacy issues**	**Privacy issues**	**Privacy issues**
Privacy laws	Privacy	Privacy	Not have it at all (privacy issue)
Perception of reduction in privacy	Privacy issues	Invasion of Privacy	Invasion of privacy GPS Tracking 24/d
Privacy objections-Strong	Invasion of privacy (body space)	Privacy Human Dignity, Individuality	Privacy – GPS
Privacy Issues	People want to retain their privacy this is an evasion of that	Invasion of privacy	Privacy issues (What Info is Not Required)
Privacy Restrictions	Privacy of Information	Privacy	Privacy Concerns
Complete Invasion of a person privacy	Perceived loss of privacy	Fear of embarrassment- you are over the Limit	Issues of confidentiality
Security of well-being in monitoring password			

Appendix 3.6 Health issues

Health issues	Health issues	Health issues	Health issues
Death	Health hazards from inserting a foreign object	Possible health issues	Illness Factors
Sickness	It's an invasive procedure	Injuries to Area	Rejection by the personal system/body
Medical	Fear of disease / Illness due to Implants	Possible Health Issues	Perceived health issues (limits take up Potential)
Allergies	Sensitivity to foreign body Under Skin	Increased Violence re increased information availability	Accidents
X-rays			

Appendix 3.7 Human issues

Human issues	Human issues	Human issues	Human issues
Human Error	Negligence	Incompetence	Incorrect Interpretation of information
Sounds difficult to do	Distance- Small communities not well informed	Market acceptance & ability to Use	Pain on Insertion
Duress in use of Mark	Implantation procedure	Resistance to the injection	Physical location of the "Mark" on the body
It Hurts	Fear of unknown to take implants in first place		

Appendix 3.8 Security issues

Security issues	Security issues	Security issues	Security issues
Concerns about security	Security	Security	Security
Security of Mark	Data security	Security of Mark	Overall personal security
Ability to remove or tamper with marks	Password		

Appendix 3.9 Cost issues

Cost issues	**Cost issues**	**Cost issues**	**Cost issues**
Cost of Scanning	Cost of implementation	Cost of equipment for Business	Hardware requirements expensive
Business acceptance - Eg Rollout Times & Cost	Admin	Cost	

Appendix 4 Perceived usefulness (open question)

Appendix 4.1 Medical issues

Medical issues	Medical issues	Medical issues	Medical issues
Form Of Identity Check- When unconscious, Etc - For Medical Emergencies Lost or Disoriented etc	Hidden Sickness will be known	Identification of medical conditions Viz	Medical Alert
Blood Type, Allergies & adverse medical conditions would be available without need for Pathology	Medical & Licensing history	Updating of Medical Position/Condition- How?	Personal Information readily available (Medical Records)
Medical History	Medical History	Medical Information & New Location	Medical Information
Ability for medical personnel to access & Determine possible ailment and treat on the spot.	Full Medical records Portability	Health Details	IF I suffered from dementia it would be useful
Update Medical history on the spot	Medical ID Blood Group	Personal Information readily available (Medical Records)	Medical History for Emergencies
Emergency Situations	Treatment of unconscious patient	Medical Emergency or Accident	Medical Emergencies
Urgent Medical treatment	Accidents	Accident	Specific Health Issue
Medical	Enhance provision of Health	Medical Care Provision	Medical
Health	One would want to be safe that in releasing ones medical information		

Appendix 4.2 Identity issues

Identity issues	Identity issues	Identity issues	Identity issues
Proof of Identity	Ability to identify "holder" of Mark if unable to communicate	Not required different ID for Different purposes	Proof of Identity
Case of Identification	For Identifying Individual	Identification	Could Be Useful In situation Where I.D Required
Name, Date of birth, Gender, Address, Age, DNA	ID	Note Question 18 "If the person's Nationality, Gender, Medical and Other relevant details were accessible on a real time basis via the "Mark" and a scanner then this would be useful Exceedingly uncomfortable scenario	Personal Identification (Airport Etc)
Locating a Missing person	Ease of locating people who are missing	Tracking Missing persons Via GPS	Missing persons Identified
Emergency Identification	Accessible in an Emergency When travelling information would be available about the person even if their belonging & ID was stolen	Form Of Identification- with Visa /M'Card etc transaction	Form of Identification- Eg Banks, Legal Circumstances
Policing Identification	A persons prior employment/ Criminal history could be available		

Appendix 4.3 Security issues

Security issues	Security issues	Security issues	Security issues
Security	Security (If Password Used)	Identify personal details, then would be useful in preventing Terrorist's Attack.	Terrorism- Stamping out knowing suspects
A "Mark would be useful for the customs security system to	You cannot Cheat	Illegal access to your Records	Cross Check- To use a, Say ticket at sports or theatre which is "Marked" to the Mark I.D.
Individual Personal security improved at Organised Functions	Security access to home/office/car	Security at Home - They are who they say they are	Unauthorised Access to Info
One would want to be certain that in releasing information to an appropriate user they could not access other information eg here's my credit card no but I don't want you to know my account balance & you would want to release certain info to your employee (Vice Versa)	One would not like releasing one's financial information (Visa Versa)	Risk Of Card/Data Loss Reduces Misuse	

Appendix 4.4 Recording issues

Recording issues	Recording issues	Recording issues	Recording issues
Personal Finances	Planning & Managing financial Info	Judging your own cash flow	Personal History Generally
Personal Budgets (Cash Flows)	Finance	Permanent Record	Consolidation of Personal Information
Improve accuracy of information provided	Accuracy	Capacity	Availability & Timeliness will improve with elimination of lost or piece meal information
Information would always be accessible	Reduces impact of Forgetfulness	Data available to professional	It's OK to collect the info its interpretation of the information (this is issue now) For agents.

Appendix 4.5 Access issues

Access issues	Access issues	Access issues	Access issues
Access	Ability to Access	Instant access to data	Always have the Information with you
Portability	Portability of Information	Convenience of use	Can't lose it?
Wouldn't be able to loose it	Instant access to Ten Bank Accounts numbers etc	NO Necessity to carry Credit Cards	Transfer of person data for self download eg When travelling
Travel	Remote Location		

Appendix 4.6 Ease issues

Ease issues	Ease issues	Ease issues	Ease issues
Ease of use	Ease Of Use	Ease of performance of everyday function	Ease of Use (Convenience)
Banking transactions could be easier	Paying bills /shopping would be easier	No Need for Cash or Cards	Obtaining finance from bank
Transformation	Speed	Size	Weight

Appendix 4.7 Problems

Problems	Problems	Problems	Problems
Mark Could be copied	Mark could be stolen	Still require proof ID	Scanners do not yet have a good record of Accuracy
Govt Control	Employee Control	Generic Control	I don't think it would as it would still be subject to major computer flaws so could produce dangerously wrong information. In my 11 years in practice I have seen several examples of Bank errors. The fact is the banks do not reconcile their transactions so giving more power to their unreliable data is madness

Appendix 4.8 Privacy issues

Privacy issues	Privacy issues	Privacy issues	Privacy issues
Privacy Matters	Privacy Matters	Confidentiality	Privacy
Privacy	Invasion of Privacy	Can only think of the potential for disaster re access to misuse of private information	

Appendix 4.9 Protest issues

Protest issues	Protest issues	Protest issues	Protest issues
All Factors, I am Completely against the use of anything of this nature	All BAD	None- Better solution without the risks are available	I cannot think of any Private use that I find Acceptable
Unable to comment because I morally object to a "Mark"	If the country was ruled by a dictator it would be useful		

Appendix 4.10 Fraud issues

Fraud issues	**Fraud issues**	**Fraud issues**	**Fraud issues**
Fraud	Less Chance of Fraud	Financial Manipulation	Less Chance of Fraud
Corruption			

Appendix 4.11 Taxation issues

Control of tax receipts & Payment	Taxation	Record keeping for tax purposes	Tracking transaction info for Income Tax- if the relevant Authority Accepts and Audits the use of the "Mark"

Appendix 5 Perceived risk (control – open question)

Appendix 5.1 Privacy issues

Privacy issues	Privacy issues	Privacy issues	Privacy issues
Invasion of Privacy	Invasion of Privacy	Privacy Invasion	The Invasion of a persons privacy
It creates a perception of invasion of privacy	Loss of Privacy	Privacy only concern	Lack of Privacy
Privacy Issue	Privacy Eliminated	Privacy ****	Privacy Eliminated
Privacy	Privacy	Privacy	Right to Privacy
Secrecy	Invasion of Privacy	Confidentiality	Confidentiality
Potential for loss of Privacy	Invasion of privacy	General Invasion of privacy	Control- No Privacy
Privacy ****	No Privacy	Invasion Of privacy	No Privacy
Privacy	Privacy Issues	Privacy	Privacy****
Lack of privacy	Privacy Issues	Privacy	Loss of privacy
Privacy Invasion	Privacy	Lack of Privacy	Invasion Of personal Privacy
Loss of Individuality in security	General invasion of privacy	People can be traced when not necessary	Could partially be used as a homing device
Instant knowledge of whereabouts	Tracking	Location	"Watching"
Spending Habits	Third Parties with access to code could access	Access of Private information /Life	Who will have access??
Who should have legal access to information Public? Govt? Medical?	Access to Information	Phone calls	Info on Mark becoming publicly available
Sale of personal details to various organisations	The Personal Loss of privacy Again with all of the personal information can you imagine all of the junk Mail	Security of personal information	Should be able to assure that no unauthorised person can access your record
Unnecessary Information	Peers or organisation can demand info not currently available	Possibility that Scanner users would obtain information not involved in the transaction being scanned	Too Personal

Others Having more Knowledge of my Financial Affairs than I do	Too Personal	Knowledge of all my Details	Data is potentially too widely available
Irrelevance of certain data to particular recipients of that data (Loss of privacy)	Knowledge of all my Details	Sale of this private information	Sale of personal info
Hasslement by hackers	Viable to receive finance/credit	Viable to recover insurance	Uncertainty about who has access to my info
All bodies that take part would have access to partial or full information	I may not wish to share	Privacy issues (What Info is Not Required)	Insufficient Privacy Legislation
Authority for organisation to Access Data via records of the 'Mark	Invasion of personal information by govt & Other Bodies	Concisely that "Mark" is a invasion of Privacy and Big Brother	

Appendix 5.2 Control issues

Control issues	**Control issues**	**Control issues**	**Control issues**
Lack of Freedom	Loss of Freedom	Violation of freedom	Anything that reduces further my freedom
Personal freedom(Right to Trade without receiving mark	Loss of freedom	Lack of Freedom	They Already Do
None of this business	Loss of Individuality (Perception Of)	Personal Liberty	I Like my Independents
Loss of me as an individual I become a thing -A statistic i.e. a computer	Control	We already have too many controls/Controllers	Control by others
Controlling my Life	This is a Control Issue	Lack Of Control	Employee Control
Generic Control	Control and Access to imp in me	Control	Control****
Abuse of Control	My Life would be totally controlled by them	My personal control is diminished	There is too much "Control" Already
Lack Of Privacy-	Control Over who	Ability to control	Information

Who Controls the Information?	has Access to the Information	/Limit Extent of Recording/Memory	control For Example the Internet was supposed to increase communication & available information the government in the name of anti spamming has introduced laws that severely now limit or freedom of speech over the Internet This also limits our sources of information to the monopolies that own the press. Look at the propaganda they have given us over the last couple of years Children overboard etc
Accountable to another authority unacceptable	Coercion	Overregulation by Govt	Government control
Government intrusion/Control taxation	Govt Control	Government have over my life	Government would have too much Control
I don't trust Government or Big Business any system which removes Personal judgment or replaces it with automation or process has to be carefully considered	Excessive Regulation	Financial & Affiliation matters should be kept at arms length from the ability of Government & Big Business.	Your choices are your business & should not be sacrificed to allow govt/big business to cost cut and over market product or implement social control function
Big Brother	The Big " Brother Issue" relating to the government	Big Brother issue	Concisely that "Mark" is a invasion of Privacy and Big Brother
Read a few George	To Much BIG	Big Brother	Plus Used to steal

Orwell books we don't need to re-visit the "Australia Card"	Brother	watching real time judgments	your Life (Big Brother)
Big Brother	Big Brother	Big Brother******	Image of Big Brother Control
Big Brother	Companies have access to information Eg Life Assurance, genetics, Banks have even greater control over us. Information not controlled by individual eg Hackers	Company control of marketing programs etc based on previous spending	Decision by entities without my knowledge
other private organization have over my life	Spending/Income - One database	The Banks have over my life	Financial Organisation may control my life
Restricts Business opportunity	Finishing up on monitoring lives-unsolicited correspondence & approaches		

Appendix 5.3 Misuse issues

Misuse issues	**Misuse issues**	**Misuse issues**	**Misuse issues**
Monitoring by undesirable persons	Safety	Exploitation by Government	Government Abuse
Incorrect use or Interpretation of information by Bureaucratic Types	Unauthorised Scanning/Interrogation of mark 'Auschivity' tag	Misuse of Information by government & Corporate sectors	Exploitation by private industry
Private sector abuse	Improper use by Private sector	Unauthorised use of info	Unauthorised Access
Authorised access/Unauthorised	Access of Information by Non authorised Interest	Access to Data restricted by Non Authorised	Unauthorised access
Any Reader can Download more data than authorised.	Information being used by unauthorised persons or in an unauthorised manner	Unauthorised Data access + Security risk	Misuse of my personal information
Security	Security	Security	Lack of security
Security of personal information	Data rerouted in download	Misuse of Information	Misuse of Data

		Scanned	
Misuse of Information	Abuse of Information	Abuse of Information	Access to personal data that could be used illegally
Fraud	Financial Manipulation	Fraud corruption of somebodies "Mark" Data	Fraudulent use (by Substitution)
Improper use	Targeted by Scam Artist	All info recorded in the Mark could be easily "Stolen"	Identity theft
Money theft	Money theft		

Appendix 5.4 Marketing issues

Marketing issues	**Marketing issues**	**Marketing issues**	**Marketing issues**
Spam style Marketing	The Marketing of products is bad enough now	Potential for marketers to "Suffocate" society with their products	More junk Mail
Marketing/Advertising targeted at me	Receiving junk mail from unsolicited sources	Info could be used for direct marketing	Commercial advantage may be taken by some person
An industry could be developed	Dehumanising concept of Marking Raises Ethical concern		

Appendix 5.5 Rights issues

Rights issues	**Rights issues**	**Rights issues**	**Rights issues**
Should be able to have the right to refuse the mark	Discrimination (those with a mark & those without	Too Invasive	I Don't want it
Biblical Prophecy	All BAD		

Appendix 5.6 Physical safety issues

Physical safety issues	Physical safety issues	Physical safety issues	Physical safety issues
Invasion of your body	Safety (robbery of limb/Mark)	Life threatening if someone has technology & wants to abuse a person to gain access	Ability of someone to extract the mark and to transplant to another person
Fear of disease / Illness due to Implants			

Appendix 5.7 Management issues

Management issues	Management issues	Management issues	Management issues
Management	Need for updating of information regularly	Probably too costly to administer	Require inputting of codes or authorised for parties to use the "Mark"

Appendix 6 "Other" Risks (open – question)

Appendix 6.1 Misuse issues

Misuse issues	Misuse issues	Misuse issues	Misuse issues
F Blackmail	Fraud	Fraud	Fraud
Fraud	Fraud	Fraud	Fraud will be easier to commit
New ways of committing fraud being discovered	Fraud, theft- same as Credit Cards, Notes	Theft	Theft
Theft	Abuse	Abuse	Abuse of intended use
Black market an manipulation	Unauthorised usage	People would trust it too much. This dishonesty associated with it would be less detectable. You can buy a machine to program sim cards from the Post office for about $65. Do you suggest that criminals would not remove the implant "Marks" There's always a chance of impostors or a thief accessing	Tampering
Security	Breach of security	Private co's using info	
Far more than just having a credit card stolen	Racial	Discrimination - Racial	Discrimination - Financial
Discrimination - Political	Too easy for people to access information	Unsupulant uses- ie marketing etc	Company Misuse- Compilation of mail list etc

Appendix 6.2 Control issues

Control issues	Control issues	Control issues	Control issues
Right ability to object against Govt policy etc could be greatly reduced or removed even though supposed rights are protected by legislation	Governments are sometimes overthrown this would allow a junta some form of population control	Legislation amendments could give grater control to government	Government Control
Place ultimate power in some hands	Lack of control of individual and God Like Abilities given to others who are probably not as competent as the individual	Control of personal activities	It is a sign of society's failure Control only leads to the need for more control. Fixing social problem is the only way
Control of personal beliefs, attitudes, etc	Less control over self	I'm not ready to become a robot yet- despite often feeling like one	Lack of acceptance uniformly & widely
Blackmail by authorities	A person's history would be too easily available & potentially deny person benefit of Changed ways- human element of judging by way person is today may be ignored - history would rule supreme	Ability to Amend	Data Changes + Manipulation of Mark
Competence	Personal freedom(Right to Trade without receiving mark	I want to live my life as I see it	Tracking of less-than-honest / moral transaction such as a brothel visit, strip club etc would be tagged
A mark would screw up my life	Loss of Individuality	Loss of Individual freedom & Anonymity	Loss of Human Independence " Marking" Ability
I would refuse to have one what are you going to do with people like me?	Not allowing it to be optional for a person	One step closer to De-Humanisation.	Possibility of segregation

Create classes of people- Outcast	Affect on future Generation		

Appendix 6.3 Health issues

Health issues	**Health issues**	**Health issues**	**Health issues**
Health	Health	Health	Personal health
Health Risk	External interference with body function by electronic means	Changes by Biological/ Physiological Actions	Fear of disease / Illness due to Implants
Poisoning of body (eg. Silicon Implants)	Body Reacts/ Rejects	Possibility of Rejection/Infection	Effect of mark i.e. Side Effect?
Getting someone else's mark by mistake infection by infection	Movement of chip in /through body	Damage through Accidents/ Injury	Self Mutilation if people seek to rid themselves of the mark
Physical assault to access	Criminal use by force	Possible assault & Theft of Mark	Crimes where the target is obtaining the chip "Mark"
A thief can amputate the mark an force to give them your password	Physical Abuse & theft of "Mark"& Transfer to thief	That part of my body would not be safe	Kidnapping/ Extortion
Steal the person not the card	Personal safety in public	People killing to obtain record via the mark	I don't fancy having a chip in my head however , However I don't see any real health issues

Appendix 6.4 Technology issues

Technology issues	**Technology issues**	**Technology issues**	**Technology issues**
Over reliance on technology	Relance on technology	Failure of technology thereby creating "duplication of people's record	System Failure- Loss of control of use of mark
Computer Error	Damage through impact	loss of ability to transact due to damage to "Mark'	I would have real concern at the possibility of mass data corruption.
Accidental damage- Vehicle or sport accident	Software is vulnerable to attack	Lack of Acceptable testing over along period and large	Reliability of Mark

		sample	
General failure (from personal experience)	Outdated information	Need for replacement/ Detection of malfunction	Wear + Tear
R+M / replacement	Technological costs and Changes	Change of technology	Future upgrade of equipment in body
Need for insertion of replacement "Mark"	Omission from the system thus creating the myriad of problems associated with getting your self "Logged" on again	People would trust it too much. This dishonesty associated with it would be less detectable. You can buy a machine to program sim cards from the Post office for about $65. Do you suggest that criminals would not remove the implant "Marks" Lose track on when individual transaction take place (i.e. Walking past a scanner) Its Possible that the "Mark would be attacked by the virus	Incorrect information could be difficult to correct

Appendix 6.5 Privacy issues

Privacy issues	**Privacy issues**	**Privacy issues**	**Privacy issues**
Privacy	Privacy	Privacy	Privacy issues
surveillance issues / Privacy issues	Privacy issues (What Info is Not Required)	Conditionality	(Perceived) Lack of Control on information
Accessibility	A person's history would be too easily available & potentially deny person benefit of Changed ways- human element of judging by way person is today may be ignored - history would rule supreme	Assist undesirable people to obtain alternative ID to avoid detection	Infringe personal barriers

Unnecessary intrusion into a person's life.	Tracking of less-than-honest / moral transaction such as a brothel visit, strip club etc would be tagged	Government using info	Private co's using info
Information being accumulated & accessed by 3rd parties	Family / Friends obtaining info		

Appendix 6.6 Identity issues

Identity issues	**Identity issues**	**Identity issues**	**Identity issues**
Identity Change	Physical assault for removal & Takeover of identity	Failure of technology thereby creating "duplication of people's record	Getting someone else's mark by mistake infection by infection being used as a guinea-pig for research etc interact adversely with computerised systems
Exchange between persons	Stereotyping		

Appendix 7 Factors affecting acceptance (open – question)

Appendix 7.1 Control issues

Control issues	Control issues	Control issues	Control issues
Beauty strength joy come from uniqueness not control & conformity	Morally unacceptable to be able to monitor people	I am loosing my Freedom	Reject because lack of freedom
Lack of personal control over who could use the mark	Freedom to choose the way I do transaction and record my life	Access to ones own Data	Lack of Guarantee mark not used to control me
Reject- My personal views communicated herein could / will be databased for someone to form an opinion on my personal traits views & perhaps habits, assuming as answers, I have been completely honest & non calculating in my answers a group of individuals could manipulate some controllable choices eg buying patterns where individuals strongly object to the control perceived or real, the history, especially in relation to Income & Expenditure, could be "muddied" by cross buying for others etc.	The notion of being Personally chipped offends my definitions of freedom & personal independence legislation would be ineffective as this does not stop theft by company employees & legislation is subject to national boundaries legislation is subject to national boundaries.	We are already stifled by too much control. This is a contributing factor to an unemployable they lack imitative because they accepted conformity. Why don't you survey people with initiative and see how many of them have got up to a bit of mischief along the really bad people will be able to overcome the mark it will just cause no end of trouble for innocent people	Freedom of movement (i.e. GPS types trucking should not be allowed) legislative controls / Limitation on who can Access the various types of data gathered from the 'Mark'
Lack of personal control over information accessible	Too much control over what we do	Lack of transparency	Encompassing all aspects of a person

Loss of control of own Identity and dealings	Centralisation & Control of personal information (reject)	Control over freedom of movement (reject)	Threat to me as an individual
Human rights lost	I fear total control over my private life	People do not want to become 'things' identified by a microchip	Overregulation by govt
Government controls at all levels are already far too high	Lack of trust in governments - reject	Government	Never trust Governments
Government controls over use mandatory moves assist acceptance	Misuses by Governments & Corporations	Government mandatory use would be rejected	When society sinks to the level of bureaucratic power I would rather be dead than accept the mark
Government may take advantage of the technology	Bureaucratic Abuse of information	Compulsory use, smacks of Big Brother attitude, incorrect use of data by both government & Corporate entities continued intrusion in form of mass marketing & Government data …	The Big " Brother Issue" relating to the government
Reject - Fear of "Big brother"	Big Brother syndrome is already too invasive in our lives	Big Brother	Being told it was compulsory
Seems if it were compulsory	Voluntary or Compulsory	Only one- my ability to turn it on and off and only have it scanned by someone I want to have scan it when I authorize that person to do so.	Compulsion would be resisted
Lack of consent	Choice is compromised	Ability to terminate "Marks" accessibility.	Unforseen uses
Restricted use of "Mark"	Legislation has not stopped Video & CD Fraud	Wrongful use of information which is irrelevant to a transaction being scanned (reject)	Completion of Financial transaction
Discrimination	None would mark me accept the mark		

Appendix 7.2 Privacy issues

Privacy issues	**Privacy issues**	**Privacy issues**	**Privacy issues**
Privacy	Privacy	Privacy	Privacy
Privacy	Privacy	Privacy	Privacy
Privacy	Privacy issue too strong	Privacy gone	Loss of privacy
Lack of privacy	Risk to privacy	Privacy concerns	Privacy Issues
Issues of privacy	Privacy issues	Privacy eliminated	Loss of privacy - reject
Perceived loss of privacy	Reject – Privacy concerns	Humans require privacy of their lives and a choice of what they discuss to whom	Personal
The Invasion of a persons privacy	Invasion of Privacy	Invasion of Privacy	Invasion of Privacy
Invasion of Privacy	There are already too many instances of invasion of privacy. Australian Taxation office, Centre Link etc.	General invasion of privacy and regulation of persons and regulation of persons existence (reject)	Privacy!!! Why should the government / business know everything I do?
I would be doubtful that security measures would be able to overcome Misuse of information and invasion of privacy	Privacy Laws	Privacy violation	Accessibility of data
Confidentiality	Issues of Violation of Freedoms	The notion of being Personally chipped offends my definitions of freedom & personal independence legislation would be ineffective as this does not stop theft by company employees & legislation is subject to national boundaries legislation is subject	Human beings should have some freedom of choice and the ability to be anonymous if they desire

		to national boundaries.	
Only one- my ability to turn it on and off and only have it scanned by someone I want to have scan it when I authorize that person to do so.	Scope of use	Perhaps I 'm just to old but I would rather the concept of a technology which while improving identification separates the person & the information Eg eye readers	The government does not appropriately control the information it currently has eg The proven hacking into ABN Registers, the proven misuse of ATO & Police information. The incorrect information shared on CRAA records etc
Individual not the record of their original position.	Reject- Complete History possible		

Appendix 7.3 Technology issues

Technology issues	Technology issues	Technology issues	Technology issues
Inherent distrust of such technology Omission from the system thus creating the myriad of problems associated with getting your self "Logged" on again	Technology Issues	Failure of technology there by creating "duplication of people's record	Reliability
Stability of records- If corrupted what are the consequences , how difficult to restore	System failure	System corruption	Risk in operation of use
Omission from the system thus creating the myriad of problems associated with getting your self "Logged" on again	Integrity of Access	Computer hackers & viruses are prevalent now and cause great stress & loss of $'s + Time This will never Change	Update capacity
Testing-	Backup	Countries Issues	Multiple implants

Widespread	identification methods		possibility one for transactions one for centre link one for police.
Not trust worthy or system need to be in place & be trust worthy	Personal attendance required for every transaction	Whilst the chip being implanted appears relatively easy the likelihood is that system to support its use will be cumbersome. Capital intensive and operation impossible and therefore perceived beliefs will be lost.	** Impossible
It would not work!!!!!!			

Appendix 7.4 Misuse issues

Misuse issues	**Misuse issues**	**Misuse issues**	**Misuse issues**
I would not accept it until I knew the reasons for it and was confident that it could not be abused. Unfortunately I do not think this sort of technology can be assured any type of type of guarantee that it will be used in a positive, legitimate way.	Ease of misuse corruption	Misuse of information and invasion of privacy	Issues of Abuse
Possibility of fraud	Fraud	Fraudulent use	Ability to external parties obtaining unauthorised access is a worry
Integrity of users	Abuses by third parties	Whilst I trust 95% of the population there is always an element of the population that cannot be trusted and the temptation to abuse this	Compulsory use- Smacks of Big Brother attitude, Incorrect use of data by both government & Corporate entities Continued intrusion

		technology for their own benefits would be too great	in form of mass marketing & Government data
Misuses by Governments & Corporations	Lack of Business Ethics	Never trust Big Business	Lack of trust in private industry-reject
I cannot think of any Private user that I find Acceptable the Banks have over my life other private organization have over my life	Abuse / Misuse Never trust Banks	The notion of being Personally chipped offends my definitions of freedom & personal independence legislation would be ineffective as this does not stop theft by company employees & legislation is subject to national boundaries legislation is subject to national boundaries.	Legislation has not stopped Video & CD Fraud

Appendix 7.5 Health issues

Health issues	**Health issues**	**Health issues**	**Health issues**
health & wellbeing	Health	Health	Health
Health Risks	Health concerns	Health Concerns	Unhealthy
Health – Lifelong implant considerations	Conclusive medical opinion as to safety issues	Personal Safety	Safety
No guarantee killer drug not implanted to be triggered if certain age reached medical condition diagnosed or wrong political party chosen.			

Appendix 7.6 Belief issues

Belief issues	Belief issues	Belief issues	Belief issues
Against my Beliefs	My Belief	Religious beliefs	No other reasons religious convictions (:the Beast syndrome)
Additional notes attached (Ref the New testament) Revelation 13:11, 16:13 "Then I saw another beast… it causes all, both small and great both rich and poor both free and slave, to me marked on the right hand or the forehead, so that no one can buy or sell unless he has the mark, that is the name of the beast or the number of its name. This calls for wisdom: let him who has understanding reckon the number of the beast, for it is human number, its number is 666	Conviction	Immoral	Has the ethics Chairperson approved of marking the Questionnaire?
Complete reversal of all Laws of human nature.	Personal		

Appendix 7.7 Just no

Just no	**Just no**	**Just no**	**Just no**
Death or the Mark ------I choose Death	I would never accept it only an arsehole would.	Nothing Could Make me accept such a mark	I wouldn't accept the "Mark"
Accept none ****	None would make me accept the mark	Just No thank you	I would strongly oppose the introduction of a mark and even change the party I vote for. I have never voted for a different party. This single issue would decide my decision
Don't like the idea of a implant			

Appendix 7.8 Security issues

Security issues	**Security issues**	**Security issues**	**Security issue**
Security	Security	Security	Security
Security of downloaded Information	Advantages over other methods of transacting Eg : Security	Personal security of finances	Case of establishing Security controls

Appendix 7.9 Humanity issues

Humanity issues	**Humanity issues**	**Humanity issues**	**Humanity issues**
We have gone far enough without further degrading humanity	Convincing positive argument for the concept required Ultimate case for humanity demonstrated	Society/ Humanity not advanced enough yet- reject	we are too anxious to revolutionise age old customs unnecessary
Let's use the technology to inform the life style of others.	Unnecessary intrusion into a persons life		

Appendix 7.10 Logic issues

Logic issues	Logic issues	Logic issues	Logic issues
Logic	Uses	Research	Burden of use outweighs any perceived benefit
Such test without wholesale adoption & implementation it will not be readily accepted			

Appendix 7.11 Convenience issues

Convenience issues	Convenience issues	Convenience issues	Convenience issues
We should be bar-coded (or Marked) At birth to get rid of TFN, ABN, Medicare Card,	Health Insurance cards, AMEX, Diners M/Card B/Card etc…etc…	Advantages over other methods of transacting	Ease of use
Pain having it inserted			

Appendix 7.12 Uniqueness issues

Uniqueness issues	Uniqueness issues	Uniqueness issues	Uniqueness issues
Destroys one's uniqueness as a human being	Loss of Individuality	Loss of Individual freedom & Anonymity	Accept - ID benefits

Appendix 7.13 Benefits issues

Benefits issues	Benefits issues	Benefits issues	Benefits issues
wide acceptance-would only use it if it could be used instead of other C/cards	Cash etc not as well as those print methods	Accept- general usage business	

Appendix 7.14 Equity issues

Equity issues	**Equity issues**	**Equity issues**	**Equity issues**
More Equitable tax system (accept)	More equitable welfare system (accept)		

Appendix 7.15 Spouse issues

Spouse issues	**Spouse issues**	**Spouse issues**	**Spouse issues**
Spouse would hate the idea!	Spouse views / Influence		

Appendix 7.16 Existence issues

Existence issues	**Existence issues**	**Existence issues**	**Existence issues**
This is putting our very existence in jeopardy.			